(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年10 月31 日 (31.10.2002)

PCT

(10) 国際公開番号
WO 02/086808 A1

(51) 国際特許分類[7]: G06K 17/00, 19/073, G06F 12/14, 15/00, H04Q 7/38

(21) 国際出願番号: PCT/JP02/03789

(22) 国際出願日: 2002 年4 月17 日 (17.04.2002)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2001-118795 2001 年4 月17 日 (17.04.2001) JP

(71) 出願人: 株式会社モビリティ (MOBILTY CO., LTD.) [JP/JP]; 〒105-0001 東京都 港区 虎ノ門１丁目１６番９号 Tokyo (JP).

(72) 発明者: 榊原 辰彦 (SAKAKIBARA,Tatsuhiko); 〒105-0021 東京都 渋谷区 恵比寿西２丁目８番５号 高麗羅ビル８Ｆ Tokyo (JP). 春日 一郎 (KASUGA,Ichiro); 〒192-0373 東京都 八王子市 上柚木３丁目１０番３号－４１０ Tokyo (JP).

(74) 代理人: 鈴木 正剛 (SUZUKI,Seigoh); 〒105-0014 東京都 港区 芝三丁目２２番７号 芝ＮＫビル４階 Tokyo (JP).

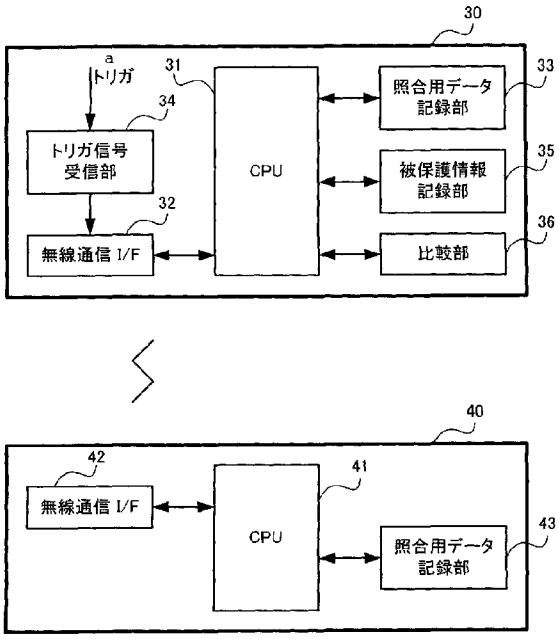
(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許

[続葉有]

(54) Title: INFORMATION PROTECTIVE SYSTEM AND INFORMATION PROTECTIVE METHOD

(54) 発明の名称: 情報保護システム及び情報保護方法



a...TRIGGER
34...TRIGGER SIGNAL RECEIVING UNIT
32...RADIO COMMUNICATION I/F
33...INQUIRY DATA RECORDING UNIT
35...PROTECTED INFORMATION RECORDING UNIT
36...COMPARING UNIT
42...RADIO COMMUNICATION I/F
43...INQUIRY DATA RECORDING UNIT

(57) Abstract: Authentication is given when first and second devices (30, 40) close to each other communicate with each other in a noncontact way, and the protected information (35) in the first device (30) is made accessible externally. After a cellular telephone (300) is brought close to a cap (400) to gain authorization, the cellular telephone (300) serving as a ticket can pass through a ticket gate.

[続葉有]

WO 02/086808 A1

(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:
— 国際調査報告書

(57) 要約:

第１の装置（３０）と第２の装置（４０）とが近傍において非接触通信を行って認証を得ることにより、第１の装置（３０）内の被保護情報（３５）に外部からアクセス可能となる。

携帯電話（３００）と帽子（４００）とを近接させて認証を得た後に、携帯電話は乗車券として改札機を通過できる。

明細書

情報保護システム及び情報保護方法

技術分野

本発明は無線通信を利用した情報保護技術に関するものである。

発明の背景

近年、市場には膨大な数の磁気カードが流通している。一例として、クレジットカード、キャッシュカード、プリペイドカード、社員証や学生証、通行証、各種証明書発行用カード、図書館の貸出カード、入退室管理カードなどがあげられる。これらのカードは特定の目的ごとに提供されているため、場合によっては外出時に何枚ものカードを携行しなければならない。しかしながら、カードの枚数によっては非常にかさばる上に、必要なときに必要なカードをすぐに取り出しにくいなどの問題がある。

これに対する対応策として、複数のカードを可能な限り１枚にまとめる方法が考えられる。たとえば、金融機関のキャッシュカードをクレジットカードとしても利用できるようにしたカードが、デビットカードとして実用化されている。デビットカードの所有者は、店舗備え付けの端末にカードを挿入して暗証番号を入力するだけで、現金を持ち歩かずに商品を購入することができる。

しかしながら、決済時にテンキーを使って自分で暗証番号を入力しなければならず、暗証番号漏洩の不安を拭いきれないことが普及の妨げとなっている。また、デビットカードでは磁気ストライプを利用しているため、紛失や盗難事故の際に改竄されやすいという問題もある。事実、磁気ストライプに記録されたデータを読み取り、偽造カードにコピーして使用する「スキミング」と呼ばれる被害が近年になって急増している。

こうしたカードの改竄や不正使用が増えている現状を背景に、磁気カードからＩＣカードに切り替える動きが各業界において本格化しつつある。周知のように、ＩＣカードとはプラスチック製のカードにＩＣチップを埋め込ん

だもので、磁気カードに比べて偽造が難しいという利点がある。また、データ記録容量が極めて大きいため、複数のカードを１枚にまとめた多目的カードを比較的容易に製造することができるという利点もある。

しかしながら、従来のクレジットカードなど個人情報と金銭的価値の両方が付帯するカードの場合、所有者以外の第三者に不正使用された場合の被害は甚大である。一方、金銭的な価値がありながら匿名性の高いカード（プリペイドカードなど）では、紛失や盗難事故の際に所有者の手元に戻ってくる可能性が極めて低いという欠点がある。さらに、金銭的な価値はなくとも個人情報が多く記録されたカード（住民カードや保健医療カードなど）であればプライバシー保護の観点からさまざまな問題が危惧される。

そこで、携帯電話、ＰＨＳ、携帯情報端末（ＰＤＡ）、ノートパソコンなどの携帯端末に多目的ＩＣカードを統合したり、複数のＩＣカードの機能を搭載したり、あるいは搭載可能な仕組み(ＩＣカードとしての機能を実行するためのソフトを所定のサーバ等にダウンロード可能な形態で提供し、そのソフトをダウンロードする、あるいはこのようなソフトが搭載された、カード用専用チップを装着する等)を用意するなどし、この端末に対してセキュリティ対策を施す方法が検討されている。ＩＣカードには大きく分けて接触型と非接触型の２種類があり、カードに記録されたデータを利用するには接触型の場合は専用の端末（以下、「リーダライタ」と呼ぶ）にカードを挿入しなければならないが、非接触型ではその必要がなく、リーダライタにかざすだけでよい。したがって、携帯端末をパスワードで保護し、端末にあらかじめ記録されたパスワードと所有者が入力するパスワードとが一致した場合にのみＩＣカードの機能を利用できるようにする方式が考えられる。しかしながら、このような方式ではカード機能を利用するたびに端末にパスワードを入力しなければならない煩わしさがあり、リーダライタにかざすだけでよいという非接触型ＩＣカードの利点が半減してしまう。また、パスワード自体は所有者個人を特定する手段にはならず、何らかの理由でパスワードが漏洩した場合に、悪意の拾得者が不正入手したパスワードを利用して端末にアクセスする可能性もある。

あるいは、携帯端末の紛失時に通常の電話機を利用して遠隔地から携帯端末を緊急制御する方法も考えられる。すなわち、プッシュボタン操作によって生成される信号を利用して携帯端末の不正使用を防止するものである。しかしながら、この方法では遠隔操作に対応した基地局の存在が不可欠になるため、確実に不正使用を防止するという意味では不十分である。

本発明は上記課題に鑑みてなされたものであり、その目的とするところは、個人情報や金銭的価値のある情報を統合して管理する場合に当該情報の第三者による不正使用を確実に防止するための情報保護システムを提供することにある。

本発明の他の目的は、かかる情報保護システムを実現するための情報保護方法を提供することにある。

発明の開示

本発明の一形態に係る情報保護システムは、被保護情報が記録された第１アセンブリと、認証情報が記録された第２アセンブリとを含む情報保護システムであって、前記第２アセンブリは前記第１アセンブリからの要求に応じて非接触による情報の送信を可能にする通信手段を備えるものであり、前記第１アセンブリは、前記被保護情報に対するアクセスを受け付ける受付手段と、前記認証情報を前記第２アセンブリより受け取って認証を行う認証手段と、この認証手段による認証結果に応じて前記受付手段で受け付けたアクセスを許可又は禁止するアクセス制御手段とを備えるものである。

また、本発明の他の形態に係る情報保護システムは、その所有者を認証するための第１認証情報と被保護情報とが記録された第１アセンブリと、前記所有者を認証するための第２認証情報が記録された第２アセンブリと、前記被保護情報を読み取る情報読取装置とを含む情報保護システムであって、前記第１アセンブリは、前記第２アセンブリおよび情報読取装置との間で非接触による情報の送受信を可能にする第１通信手段を備えるものであり、前記第２アセンブリは、前記１アセンブリとの間で非接触による情報の送受信を可能にする第２通信手段を備えるものであり、前記情報読取装置は、前記第

１アセンブリとの間で非接触による情報の送受信を可能にする第３通信手段を備えるものであり、前記第１アセンブリは、さらに、前記情報読取装置からの信号に応答して前記第２アセンブリより前記第２認証情報を受け取り、受け取った第２認証情報および前記第１認証情報に基づく認証を行い、認証結果に応じて前記被保護情報の前記情報読取装置による読み取りを許可又は禁止する手段を備えるものである。

本発明の一形態に係る情報保護システムにおいては、認証手段を第２アセンブリ、又は、第１アセンブリと第２アセンブリとの双方に設けても良い。これらの第１アセンブリ、第２アセンブリは、いずれも、単独で携帯可能であるか、または携帯可能な製品に内蔵された形態で提供することが可能である。

前記通信手段における通信形態には特に制限はない。例えば、前記通信手段は、電磁誘導による無線通信、電磁結合による無線通信、静電結合による無線通信、マイクロ波帯の周波数を用いた無線通信、及び光を情報の搬送媒体とする通信、のいずれかによって通信を行う構成とすることができる。

また、前記第１アセンブリおよび前記第２アセンブリを、それぞれ非接触通信用のアンテナを含むＩＣモジュールとして提供してもよい。

前記第１アセンブリの形態としては、カード媒体に埋め込まれた形態、シート状の媒体に埋め込まれた形態、携帯性端末に内蔵された形態、データキャリアに内蔵された形態等が挙げられる。

前記第２アセンブリは、好適には、前記第１アセンブリを所持する者が常に持ち歩くもの、より好適には第３者が容易に盗むことができないものとする。例えば、前記第１アセンブリを、所持する者が身につける装飾品、例えば指輪に埋め込むことができる。

また、本発明の他の形態では、前記アクセス制御手段は、当該認証手段でアクセスを許可するという認証結果が得られた場合は、前記アクセス要求から所定時間が経過するまでは、被保護情報へのアクセスを許可する。

また、第１、第２のアセンブリは、集積回路アセンブリとして提供することも可能である。

図面の簡単な説明

図１は、本発明の一実施形態による情報保護システムの概要を示すブロック図である。

図２は、ＩＣアセンブリ３０へのアクセス要求に対してのＩＣアセンブリ３０のＣＰＵ３１における認証処理を表すフローチャートである。

図３は、多目的携帯端末３００とＲバッジ４００の説明図である。

図４は、自動改札機に非接触型ＩＣカード用のリーダライタ５０を設けた例の説明図である。

図５は、ＲＦＩＤインターフェースを備えた携帯端末の構成を表す図である。

図６は、複数のＲＦＩＤインターフェースを備えた携帯端末の構成を表す図である。

図７は、携帯端末のソフトウェアの構成を表す図である。

図８は、ＩＣカードの構成を表す図である。

図９は、電磁誘導による送受信の仕組みを示す図である。

図１０は、データを受信の動作を表すフローチャートである。

図１１は、データを発信の動作を表すフローチャートである。

図１２は、個別情報システムの構成を表す図である。

図１３は、携帯端末に個別情報が格納されているようすを示す図である。

図１４は、個別情報システムの動作を示すフローチャートである。

図１５は、使用者識別システムの構成を表す図である。

図１６は、レッドバッジの例を表す図である。

図１７は、レッドバッジの例を表す図である。

図１８は、レッドバッジの例を表す図である。

図１９は、レッドバッジのＩＣチップの構成を表す図である。

図２０は、識別情報を登録する動作を表すフローチャートである。

図２１は、識別情報より利用可能かを判断する動作を表すフローチャートである。

図２２は、レッドバッジを個別情報システムで利用した図である。

図２３は、携帯記録素子書込システムの構成を表す図である。

図２４は、携帯記録素子書込システムの動作を示すフローチャートである。

図２５は、携帯記録素子書込システムでレッドバッジを利用した図である。

図２６は、管理システムの第１の構成を表す図である。

図２７は、利用管理システムの第１の動作を表す図である。

図２８は、携帯端末に表示される画面の例である。

図２９は、第１の利用管理システムでレッドバッジを利用した図である。

図３０は、利用管理システムの第２の構成を表す図である。

図３１は、利用管理システムの第２の動作を表す図である。

図３２は、携帯端末に表示される画面の例である。

図３３は、第２の利用管理システムでレッドバッジを利用した図である。

図３４は、携帯端末の間で送受信の行われる様子を示す図である。

発明を実施するための最良の形態

＜概略構成＞

以下、本発明の実施形態を図面を参照して説明する。

図１は、本発明の一実施形態による情報保護システムの概要を示すブロック図である。この情報保護システムは、第１のＩＣアセンブリ３０と第２のＩＣアセンブリ４０とで構成される。第１のＩＣアセンブリは、中央処理装置（ＣＰＵ）３１と、無線通信インタフェース部３２と、照合用データ記録部３３と、トリガ信号受信部３４と、被保護情報記録部３５とを備えている。同様に、第２のＩＣアセンブリ４０は、ＣＰＵ４１と、無線通信インタフェース部４２と、照合用データ記録部４３とを備えている。また、第１および第２のＩＣアセンブリ３０および４０は、各アセンブリで必要なアプリケーションプログラムや制御プログラム、オペレーティングシステム（ＯＳ）、デバイスドライバなどが格納された図示しない読取専用メモリ（ＲＯＭ）やランダムアクセスメモリ（ＲＡＭ）を含む。

第１のＩＣアセンブリ３０および第２のＩＣアセンブリ４０は、無線を利

用して互いにデータの送受信が可能なように構成されている。この場合、本願明細書において使用する「無線通信」という用語は、金属端子による電気的な接触を使用せずに行う通信全般を意味し、一例として、非接触自動識別システム（ＲＦＩＤ:Radio Frequency Identifycation）で用いられている電磁結合方式、電磁誘導方式、マイクロ波方式、光方式の無線通信があげられる。また、米国特許第６，２１１，７９９号（特開平１１－２２５１１９号）に開示されているような人体を介して電力と情報を伝送するための方法による通信も本願明細書における「無線通信」に包含されるものとする。

ＣＰＵ３１は、第１のＩＣアセンブリ３０の各構成要素を制御し、ＣＰＵ４１は第２のＩＣアセンブリ４０の各構成要素を制御する。無線通信インタフェース部３２および４２は、それぞれが送信機能と受信機能の両方を有する。この無線通信インタフェース部３２および４２は、たとえばＲＦＩＤ技術において用いられているようなアンテナやコイルなどを有し、互いにデータの送受信を行うものである。

ＲＦＩＤにはさまざまな変調方式や周波数、通信プロトコルを利用したものがあるが、本発明は特定の方式に限定されるものではなく、どのような方式を利用してもよい。ＩＣアセンブリに設けられる無線通信インタフェース部の数にも特に制限はなく、必要に応じて異なる変調方式で機能する無線通信インタフェース部を複数設けるようにしてもよい。なお、汎用性の観点から見ると、非接触型ＩＣカードの分野で標準規格化が進められている仕様に準拠するなどの方式を採用すると好ましい。日本においては、次世代ＩＣカードシステム研究会（ｔｈｅ Ｎｅｘｔ Ｇｅｎｅｒａｔｉｏｎ ＩＣ Ｃａｒｄ Ｓｙｓｔｅｍ Ｓｔｕｄｙ Ｇｒｏｕｐ）やＩＣカードシステム利用促進協議会（Ｊａｐａｎ ＩＣ Ｃａｒｄ Ｓｙｓｔｅｍ Ａｐｐｌｉｃａｔｉｏｎ Ｃｏｕｎｃｉｌ）が標準化活動を行っている。また、すでに確立されている国際規格として、ＩＳＯ／ＩＥＣ１０５３６、ＩＳＯ／ＩＥＣ１４４４３、ＩＳＯ／ＩＥＣ１５６９３がある。このような規格に準拠した無線通信インタフェース部３２および４２とすることで、より一層汎用的かつ実用性の高い情報保護システムを構築できる可能性がある。

照合用データ記録部３３および４３には、第１および第２のＩＣアセンブリの照合を行うためのデータが記録されている。この照合用データが所定の条件を満たした場合に限り、被保護情報記録部３５へのアクセス、例えば被保護情報記録部３５に格納されたデータやプログラムへのアクセスが許可される。照合用データとは、ＩＣアセンブリの所有者を一意に特定するためのデータであり、その内容は特に限定されるものではない。たとえばＣＰＵの固有記号や製品番号、クレジットカード番号、これらの一意なデータを複数組み合わせたものや、さらにこれを暗号化したものなどを照合用データとして利用することができる。被保護情報とは、個人情報や金銭的価値のある情報など、ＩＣアセンブリの所有者が第三者による閲覧や使用を制限し、保護することを希望する情報またはデータであれば、どのような情報またはデータであってもよい。一例として、クレジットカード、キャッシュカード、プリペイドカード、各種会員権、診察券、健康保険証、身分証明書、公共施設のチケットなど従来のカード類に記録されたデータの他、電子マネーや電子取引情報、私的な住所録やドキュメント、画像データなど、さまざまなものが考えられる。

図２に、ＩＣアセンブリ３０へのアクセス要求に対してのＩＣアセンブリ３０のＣＰＵ３１における認証処理を表すフローチャートを示す。

無線通信インタフェース部３２は、トリガ信号受信部３４と接続され、後述するトリガ信号を受信する。ＣＰＵ３１は、トリガ信号受信部３４でトリガ信号が受信されないときは、ＩＣアセンブリ３０に対するアクセス要求は無しと判定し、トリガ信号が受信された場合はアクセス要求有りと判定する（Ｓ１１）。トリガ信号が検出された場合、ＣＰＵ３０は、無線通信インターフェース３２を通じて、当該トリガ信号に応答して第２のＩＣアセンブリ４０に対して照合用データの送信を要求する要求信号を送信する（Ｓ１２）。第２のＩＣアセンブリ４０は、この要求信号に応答して、自己の照合用データ記録部４３に格納された照合用データを第１のＩＣアセンブリに送信する。ＣＰＵ３１は、無線通信インターフェース３２を通じて照合用データが受信されたか否かを判定し（Ｓ１３）、受信さない場合はアクセスを拒否す

る（Ｓ１４）。照合用データが受信された場合、ＣＰＵ３１は、第２のＩＣアセンブリ４０から受信した照合用データとＩＣアセンブリ３０の照合用データ記録部３３に格納された照合用データとの比較処理を開始させる（Ｓ１５）。この例では、この比較は、比較部３６によって行われる。

比較部３６における比較の結果、所定の条件が満たされたか否かを判定する。この例では、ＩＣアセンブリ４０から受信したデータとＩＣ照合用データとが一致するか否かを判定し（Ｓ１６）、一致した場合には、ＣＰＵ３１は、アクセスを許可し（Ｓ１７）、被保護情報記録部から必要な情報を抽出する。一方、所定の条件が満たされなかった場合は、ＣＰＵ３１は被保護情報記録部３５に格納されたデータへのアクセスを禁止する（Ｓ１４）。

照合用データ記録部３３、４３、被保護情報記録部３５などの記録部は、たとえばＩＣチップなどの記録素子で実現される。なお、図１に示す例では照合用データの比較を第１のＩＣアセンブリ３０において行ったが、第２のＩＣチップアセンブリ４０側で比較を行うことも可能である。この場合、比較を行った後に第２のＩＣアセンブリ４０から第１のＩＣアセンブリ３０に比較の結果を無線通信にて通知し、ＣＰＵ３１は当該比較の結果に応じて被保護情報記録部３５へのアクセスを許可するか否かを判断する。あるいは、第１のＩＣアセンブリ３０と第２のＩＣアセンブリ４０の両方に比較部を設け、異なる照合用データをやり取りして双方で所定の条件が満たされた場合にのみ被保護情報記録部３５へのアクセスが可能なような形態にしてもよい。特に後者のような二重照合形態にすることで、被保護情報記録部３５に格納されたデータを一層確実に保護することができる。

上述した第１および第２のＩＣアセンブリは、周知の半導体製造技術を用いて製造可能なものであるが、本発明は半導体による集積回路に限定されるものではない。たとえば、光電子集積回路（ＯＥＩＣ）やバイオ系チップを用いて第１および／または第２のＩＣアセンブリを製造してもよい。このようにして製造したＩＣアセンブリは、小型チップとしてさまざまな物体に埋め込むことが可能なものである。以下、本発明の目的において、ＩＣアセンブリを装飾品や衣類など所有者の身近におくことが可能な物体に埋め込ん

だものを「Ｒバッジ」と総称する。また、個人情報や金銭的価値の付帯する情報を携帯端末に統合したものを「多目的携帯端末」と総称する。

次に、図３を参照すると、第１のＩＣアセンブリを多目的携帯端末３００の形で実現し、第２のＩＣアセンブリをＲバッジ４００の形で実現した例が示されている。多目的携帯端末３００はスイッチ３０１を備え、端末の所有者がスイッチ３０１を押すことでトリガ信号が生成される。トリガ信号受信部３４（図１）は、トリガ信号を受信すると、無線通信インタフェース部３３に対して第２のＩＣアセンブリとの間での通信を開始するよう指示する。これ以降の照合動作については図１を参照して説明したとおりである。このようにすることで、多目的携帯端末とＲバッジとの間で照合用データを照合し、照合の結果が所定の条件を満たした場合に限って多目的携帯端末を使用可能とすることができる。

図４は、自動改札機に非接触型ＩＣカード用のリーダライタ５０を設け、このリーダライタから送信される信号（プリチャージ信号）をトリガ信号として利用した例を示している。この場合、リーダライタから発信される信号は、周知のＲＦＩＤシステムにおいて利用されている信号と同様のものである。利用者が多目的携帯端末３００を自動改札機に近づけると、リーダライタ５０から発信されるプリチャージ信号に応答して多目的携帯端末３００がＲバッジ４００との通信を開始する。これ以降の照合動作については図１を参照して説明したとおりである。利用者は多目的携帯端末を自動改札機に近づけるだけで、改札を通ることができるという利点がある。自動改札機に限らず、金融機関のＡＴＭや公衆電話など、決済や金銭の移動を伴う行為に関わる多くの設備に同様の方式を応用することが可能である。

また、照合結果が所定の条件を満たした後所定時間が経過する前に被保護情報へのアクセスがなされた場合はそれを許可し、この所定時間が経過した後の場合はアクセスを禁止するようにしてもよい。この場合、例えば、ＩＣアセンブリ３０または４０のいずれか一方または両方にタイマを設けることで、上述のような所定時間が経過したか否かを検出することが可能となる。このような方法をとることで、ＩＣアセンブリ３０と４０との間の距離が通

信可能距離よりも長い場合であっても本発明を実現することが可能である。

以下、多目的携帯端末３００に乗車券を統合して自動改札機を通過する場合を例に説明する。なお、この例では、多目的携帯端末３００（ＩＣアセンブリ３０）とＩＣアセンブリ４０との間の通信可能距離が１０ｃｍであるものとする。通常の自動改札機においては、多目的端末３００を手で保持した状態で自動改札機のリーダライタ５０に近づけて認証を行う。ＩＣアセンブリ４０が例えば指輪に実装されているのであれば、多目的端末３００内のＩＣアセンブリと指輪との間隔は１０ｃｍよりより短いので、問題なく認証を行うことができる。しかし、ＩＣアセンブリ４０が帽子あるいはイヤリングに実装されている場合、ＩＣアセンブリ３０とＩＣアセンブリ４０との間の距離は、通常は１０ｃｍよりも長くなり、認証を行うことができなくなる。

このような場合、多目的携帯端末３００を帽子あるいはイヤリングに近づけてＩＣアセンブリ３０とＩＣアセンブリ４０との距離を１０ｃｍ以下としたうえで、ＩＣアセンブリ４０とＩＣアセンブリ３０との間での認証を行わせる。この動作は、例えば図３の例では、多目的携帯端末３００を帽子またはイヤリングの近傍に持っていった状態で、多目的携帯端末３００のスイッチ３０１を押してトリガ信号を発信させることにより認証を行う。

また、図４の例では、リーダライタ５０から発信されるプリチャージ信号に応答可能な範囲内に多目的携帯端末３００がある状態で、多目的端末３００を耳元に近づけて帽子又はイヤリングに実装されたＩＣアセンブリ４０との距離を１０ｃｍ以下とすることで、認証を行い、携帯端末３００に記録された乗車券のデータを利用可能とすることができる。このように、タイマを設けて一定のタイムラグを許容することで、ＩＣアセンブリ３０とＩＣアセンブリ４０とを実際に使用するときの距離が比較的長い場合であっても、通信可能距離の短い通信方式を採用することが可能になる。

また、携帯端末に保存された情報を、専用のサーバにバックアップしたり、仕様内容のログファイルを保存することにより、それらの情報を必要に応じてダウンロードし、紛失前の状態に復帰できるようにしてもよい。

更に、所有者はＩＣカードをそのまま使うかＩＣカード機能を内蔵した携

帯端末として使うかを選択することができる。さらに、ＩＣアセンブリ３０に周知のＧＰＳ機能を内蔵させることで、ＩＣアセンブリ３０を紛失したようなときにも被保護情報記録部３５に記録されたデータに対する保護性を一層高めることができる。

次に、本発明を端末等に適用した実施の形態を以下の“第１の実施の形態”～“第７の実施の形態”を例にとって詳細に説明する。

第１の実施の形態における携帯端末１０は、図５に示すように、電波認識方式でデータの送受信を行う送受信部２０と、ＲＡＭやＲＯＭなどからなるメモリ３０と、ＣＰＵ（中央制御処理装置）などからなる制御部４０から概略構成される。

電波認識方式とは、ＲＦＩＤなどに代表される送受信方式で、電気的な接続を行わずにデータが送受信されるもので、電磁結合・電磁誘導・マイクロ波・光などを利用したものである。

この携帯端末１０は、携帯電話、ＰＨＳ、ＰＤＡ（携帯情報端末）、ノートパソコンなどの端末である。電波認識方式で送受信するインターフェースを、以下、ＲＦＩＤインターフェースと呼ぶ。

制御部４０は送受信部２０やメモリ３０に接続して、送受信部２０やメモリ３０を制御する。

送受信部２０には、発信部（或いは、送信部）と受信部を兼ね備えたもので、アンテナ２２を介してＲＦＩＤインターフェースを備えた記録素子などからデータを読み取る機能や、記録素子などにデータを書き込む機能、或いは、ＲＦＩＤインターフェースを備えた読取装置にデータを発信する機能などを備える。

記録素子とは、ＩＣチップなどである。以下、記録素子をＩＣチップとして説明する。

また、送受信部２０は、通信制御用ＩＣなどからなる通信制御用部２１とアンテナ２２などから構成される。ここでは、通信制御用部２１を通信制御用ＩＣとして以下説明する。

さらに、送受信部２０の通信制御用ＩＣ２１は制御部４０と接続され、制

御部４０からデータを読み込むためのコマンドを受け取りアンテナを介してデータを送受信するものである。

メモリ３０は制御部４０と接続され、データを格納する部分や、ＯＳ（オペレーティングシステム）や通信制御用ＩＣ２１を制御するデバイスドライバなどの制御プログラム、さらに、アプリケーションプログラムなどを備えている。

ＲＦＩＤインターフェースには、さまざまな変調方式・周波数・通信プロトコル等がある。そこで、図６に示すように、それぞれに対応した、通信制御用ＩＣ２１やアンテナを用意し、さらに、通信制御用ＩＣ２１を制御するデバイスドライバなどの制御プログラムを携帯端末１０に複数用意して必要に応じて選択可能なように構成することもできる。

また、標準化の観点からすると、密着型としてＩＳＯ／ＩＥＣ１０５３６、近接型としてＩＳＯ／ＩＥＣ１４４４３、近傍型としてＩＳＯ／ＩＥＣ１５６９３のＲＦＩＤインターフェースを備えることが好ましい。また、キャリア周波数としては、１２５ｋＨｚ～４００ｋＨｚ、４．９１５２ＭＨｚ、１３．５６ＭＨｚ、２．４５ＧＨｚのものが考えられる。

また、ＲＦＩＤインターフェースには、例えば、一方を体に装着し一方を手に持つと人体を通して送受信することが可能なものもある。このように、伝導性のあるものを媒介にして送受信をおこなう機能を持たせることもできる。

さらに、上述したものに限らず、必要に応じて他の方式のＲＦＩＤインターフェースの組み込みが可能である。

また、携帯端末１０には、図７のブロック図に示すように、各ＲＦＩＤインターフェースに対応した送受信部２０と、この各ＲＦＩＤインターフェースを利用するためのデバイスドライバ（制御プログラム）３１とを複数用意し、ＯＳ（オペレーティングシステム）などからなるシステム管理部３２上でさまざまなアプリケーションプログラム３３を動作させることができ多種多様な機能を持たせることが可能である。さらに、必要に応じて、アプリケーションプログラム３３で利用するデータを格納するデータ格納部３４

を持つ。

さらに、このアプリケーションプログラム３３やデバイスドライバ３１は、インターネットなどのネットワークからダウンロードして、新たな機能の追加や、更新することが可能である。

また、ＩＣカードにも、前述したＲＦＩＤインターフェースと同様の構成を備えている。図８に示すように、ＩＣカード５０にはＩＣチップ５１がアンテナ２２と接続されている。

記録素子であるＩＣチップ５１には、通信制御用ＩＣ２１とＣＰＵなどからなる制御部４０とメモリ３０を備え、アンテナ２２を介してデータの送受信を行う。メモリ３０は制御部４０と接続され、データをメモリに格納する部分や、通信制御用ＩＣ２１を制御するソフトウェアを備えている。さらに、ＯＳを備えるようにしても良い。

あるいは、通信制御する部分を集積回路とすることも可能である。

また、図示しないが、あらゆる装置に前述したＲＦＩＤインターフェースの送受信部２０を組み込むことができ、ＲＦＩＤインターフェースでデータの送受信を行う機能を持たせることが可能である。

次に、送受信部２０の送受信を行う仕組みについて、電磁誘導を使って送受信する例について具体的に説明する。

ここでは、図９に示すように、送受信部２０を受信部２０’と発信部（送信部）２０”とに分けて説明する。

まず、受信部２０’では、通信制御用ＩＣ２１には、制御部４０から読み取りのコマンドを受けてデータの読み取りを開始する読み取り制御部２１１と、受信したデータを制御部４０’に渡すデータ受信部２１２とを備える。

読み取り制御部２１１は、制御部４０’から読み取りのコマンドを受け取ると発信要求としてパワーパルスを発生してアンテナ２２’から送出する機能を備える。また、データ受信部２１２は、発信部２０”からのデータをアンテナ２２’で受信するとデータをデコードして制御部４０’に渡す機能を備える。

発信部２０”には、電磁誘導によるキャパシティを蓄える蓄電部２１３と、

データを送信するデータ送信部２１４と備える。

蓄電部２１３は、アンテナ２２”で受信部２０’から発信要求としてパワーパルスを受け取ると蓄電する機能を備える。また、データ送信部２１４では、蓄電部２１３に蓄えられたエネルギーを電源としてアンテナ２２”からデータを発信する機能を備える。

また、発信部２０”に、電源が接続される構成になっている場合には、パワーパルスを受信信号としてのみ利用し、蓄電部２１３を備えない構成とすることも可能である。

送受信部２０は、受信部２０’と発信部（送信部）２０”の双方の機能を兼ね備えるものである。

次に、本実施の形態の動作をフローチャートに従って説明する。

ここでは、ＲＦＩＤインターフェースを備えたＩＣカードや装置からデータを受信する場合を例に、携帯端末１０の受信の動作を図１０のフローチャートを用いて説明する。

まず、ＲＦＩＤインターフェースを備えたＩＣカードや装置などの近くに携帯端末１０を持っていく。ＲＦＩＤインターフェースを備えたＩＣカードや装置と携帯端末１０とが送受信可能な距離は、密着型か、近接型か、近傍型かによって違う。密着型か、近接型か、近傍型かは目的により使い分けられ、アプリケーションプログラムで選択されたデバイスドライバを用いて送受信を行う（Ｓ１００）。アプリケーションプログラムからデバイスドライバに読み取りのシステムコールを呼び出すと、デバイスドライバから通信制御用ＩＣ２１に読み取りのコマンドが送られる（Ｓ１０１）。通信制御用ＩＣ２１は、読み取りのコマンドを受け取ると読み取り制御部２１１を介してアンテナ２２（２２’）より発信要求としてパワーパルスを発生する。

ＩＣカードや装置は、発信要求としてパワーパルスを受け取り、電磁誘導で発生した電流は蓄電部２１３に蓄える（Ｓ２００）。蓄電部２１３に蓄えられた電力を使用してデータをアンテナ２２”から発信する（Ｓ２０１）。

携帯端末１０は、アンテナ２２（２２’）を介してデータを受信し（Ｓ１０３）、データ受信部２１２を介してデコードされたデータは、デバイスド

ライバからアプリケーションプログラムに渡される。

次に、ＲＦＩＤインターフェースを備えたＩＣカードや装置などにデータを発信する場合を例に、携帯端末１０の発信の動作を図１１のフローチャートを用いて説明する。

ＩＣカードや装置では通信制御用ＩＣ２１に読み取りのコマンドを送る（Ｓ２１０）と、ＩＣカードや装置の通信制御用ＩＣ２１は、読み取りのコマンドを受け取ると読み取り制御部２１１を介してアンテナ２２（２２'）より発信要求としてパワーパルスを発生する（Ｓ２１１）。

携帯端末１０は、発信要求としてパワーパルスを受け取ると（Ｓ１１０）、それをＣＰＵの割り込み信号として利用し、データをアンテナ２２（２２"）から発信する（Ｓ１１１）。あるいは、電磁誘導で発生した電流を蓄電部２１３に蓄え、蓄電部２１３に蓄えられた電力を利用してデータを発信しても良い。

ＩＣカードや装置は、アンテナ２２（２２'）を介してデータを受信する（Ｓ２１２）。

ここでは、携帯端末１０には送受信部に受信部の機能と発信部（送信部）の機能を備えたものについて説明したが、受信部の機能か発信部（送信部）の機能かいずれかを一方のみを備えたものでも良い。

また、ここでは電磁誘導による例について説明したが、データを受信する側から発信要求としてポーリングしてデータを受信するようにしても良い。

さらに、送受信部２０は携帯端末１０に脱着可能なユニットとし（例えば、カード型ユニットなど）、さまざまなＲＦＩＤインターフェースを装着することが可能である。

あるいは、記録素子には半導体以外のものを利用してＩＣチップと同様の機能をもつもので構成するようにしても良い。

以上、説明したようにＲＦＩＤインターフェースを備えた携帯端末１０を利用して、ＩＣカード５０とデータの送受信を行うことができる。さらに、ＲＦＩＤインターフェースを備えた装置ともデータの送受信が行うことができる。

また、携帯端末１０でＩＣカード５０や装置に記憶されている固有のデータを読み込むと、アプリケーションを起動することも可能である。例えば、ＩＣカード５０の情報を読み込むとインターネットに接続する。あるいは、ＲＦＩＤインターフェースを組み込んだ装置から情報を読み込むと、説明書などを表示することもできる。

第２の実施の形態では、携帯端末１０に（ＩＣカードで行われている）定期券・乗車券・クレジットカード・鍵などの機能を内蔵させる個別情報システムについて説明する。ここでは、クレジットカードなどカード機能を携帯端末１０に内蔵させる場合を例に説明する。前述の実施の形態と同一のものには同一符号を伏して詳細な説明を省略する。

他の実施の形態における個別情報

システム１１は、図１２に示すように、携帯端末１０とＲＦＩＤインターフェースの送受信部２０’（受信部）を組み込んだ受信装置６０とで概略構成される。

受信装置６０は、送受信部２０’と制御部４０’が設けられ、携帯端末１０から個別情報を読み取る機能を備えている。この受信装置６０に携帯端末１０を近づけて個別情報を読み取るようにするため、送受信部２０’には、近接型を使用することが好ましい。

携帯端末１０は、図１３に示すように、メモリ３０上のデータ格納部３４に個別情報３４０を記憶する。ここでは、個別情報３４０としてカード情報を記憶している例について説明する。

個別情報３４０には、複数のカード情報（例えば、図１３のＡ、Ｂ、Ｃ）を記憶することも可能でその中から利用するカードを選択する機能を備える。さらに、カードに応じたアプリケーションプログラム３３を複数用意し、各カードに応じた機能を持たせることが可能である。

以下、個別情報３４０をカード情報と置き換えて説明する。

次に、本実施の形態の動作を図１４のフローチャートに従って説明する。

携帯端末１０で、利用するカードを選択して（Ｓ１２０）、携帯端末１０

を受信装置６０に近づける。受信装置６０では、例えば、受信装置６０に設けられている読み取りスイッチの押下によって、カード情報３４０の読み取り指示を受け取ると、読み取りコマンドを送受信部２０に送る（Ｓ２２０）。そこで、送受信部２０から指定されているカードのカード情報３４０（個別情報）の発信要求（パワーパルスなど）を携帯端末１０に発信する（Ｓ２２１）。

携帯端末１０では、カード情報３４０の発信要求を受け取ると選択されているカード情報３４０を発信する（Ｓ１２２）。受信装置６０では、受信したカード情報３４０が、要求したカード情報であれば処理を続行するが（Ｓ２２４）、要求したカード情報でない場合はエラー終了する（Ｓ２２５）。

本実施の形態では、携帯端末１０にカード機能を持たせる場合について説明したが、定期券や乗車券の機能を持たせることも可能である。この場合には、受信装置６０の送受信部２０には、多少離れた位置から読み取り可能なように近接型を利用することが好ましい。

また、携帯端末１０に鍵の機能を持たせることも可能である。この場合には、受信装置６０の送受信部２０には、やや離れた位置から読み取り可能なように近傍型または近接型を利用することが好ましい。

また、電子マネー・クレジットカード・会員権・診察券・健康保健所・身分証明書・アミューズメント施設のチケット類の機能を持たせることも可能である。

さらに、個別情報３４０は、携帯端末１０の固体それぞれを識別する識別情報を利用することもできる。

さらにまた、携帯端末１０を買い換えるなど置き換えをする場合には、携帯端末１０に記録されている電子マネー・クレジットカード・会員権などを管理する管理会社にインターネットなどを介して置き換えを通知する。そこで、古い携帯端末１０では利用できないようにし、新しい携帯端末１０にその情報をダウンロードして利用するようにすることも可能である。

以上、説明したように、携帯端末１０に、複数の機能を兼ね備えるようにすることが可能である。

第３の実施の形態では、識別情報を記憶するＩＣチップを利用して携帯端末１０の使用者を識別する使用者識別システムについて説明する。前述の実施の形態と同一のものには同一符号を伏して詳細な説明を省略する。

いつも身に付けているものや身近におくものにＩＣチップを埋め込んだものを総称して、以下、レッドバッジと呼ぶ。

第３の実施の形態における使用者識別システム１２は、図１５に示すように、携帯端末１０と識別情報を記憶する携帯記録素子とで概略構成される。以下、携帯記録素子としてＩＣチップ５１とアンテナ２２を組み込んだレッドバッジ７０を例に説明する。

ここで、ＩＣチップ５１を内蔵したレッドバッジ７０の例について説明する。レッドバッジ７０は、第１のタイプとして、図１６に示すように、指輪・イヤリング等の本体をアンテナ２２として本来の目的と共用し、それにＩＣチップ５１が備えられるタイプがある。

第２のタイプとして、図１７に示すように、ネクタイピン等の本体６１にＩＣチップ５１とアンテナ２２が内蔵される。或いは、図１８に示すように、カフスボタン・バッジ・ブローチ・ペンダント・コンタクトレンズ等の本体６２にＩＣチップ５１とアンテナ２２が内蔵されたものなど身につけるものに内蔵されるタイプがある。

他にも、財布・パスケース等の本体にＩＣチップ５１とアンテナ２２が内蔵される。筆記用具・ライター等の本体にＩＣチップ５１とアンテナ２２が内蔵されたものなど身近におくものに内蔵されるタイプがある。

以上、例に挙げたものだけでなく、様々なものにＩＣチップ５１を内蔵することができアンテナ２２の形状も多様である。

また、図１９に示すように、レッドバッジ７０に内蔵されたＩＣチップ５１には、識別情報をメモリ３０の識別情報記憶部３５に格納する。識別情報記憶部３５はＲＯＭなど書換不可能な記録素子で構成されることが望ましい。また、識別情報３５０は一意に識別できるように割り振ったものである。識別情報３５０はレッドバッジ７０の製造時に、一意となるように書き込むようにしても良い。

また、携帯端末１０の近傍に複数の第３者のレッドバッジ７０が存在する場合を考慮すると、携帯端末１０とレッドバッジ７０は、近接していないと識別情報３５０が読み取れないようにするほうが望ましい。近接とは、使用している携帯端末１０と、使用者が衣類につけるなど身につけた状態のレッドバッジ７０とが送受信可能な程度である。

以上の条件を考慮に入れると、レッドバッジ７０には、近接型または密着型のＩＣチップを使用することが好ましい。さらに、レッドバッジ７０と携帯端末１０との送受信可能な範囲は数十センチメートル以下であることが望まれる。

次に、本実施の形態の動作をフローチャートに従って説明する。

識別情報３５０を登録する動作について、図２０のフローチャートを用いて説明する。以下、フローチャートではレッドバッジ７０をＲバッジとする。

まず、携帯端末１０にレッドバッジ７０の識別情報３５０を登録するための登録モードにする（Ｓ１３０）。この登録モードにする際には、暗証番号やバイオメトリックス（アイリス、声紋、指紋など）を入力しないと登録モードにならないようにし、第３者では登録できないようにする。登録モードになると、読み取り開始のコマンドを制御部４０から通信制御用ＩＣ２１に送信するとアンテナ２２から発信要求（パワーパルスなど）を発信してレッドバッジ７０の読み取りを開始する（Ｓ１３１）。

ここで、携帯端末１０のタイマーに所定の時間ｔを設定する（Ｓ１３２）。そこで、時間ｔが経過するまで（Ｓ１３４）、レッドバッジ７０から識別情報３５０を受信したか繰り返しチェックする（Ｓ１３３）。

時間ｔが経過しても、レッドバッジ７０から識別情報３５０の受信が完了しない場合は、携帯端末１０の画面上にエラーメッセージを表示する（Ｓ１３５）。或いは、受信した識別情報がすでに登録済みの識別情報の場合には、携帯端末１０の画面上にエラーメッセージを表示する（Ｓ１３５）。

受信した識別情報３５０が登録済みの識別情報でない場合は、識別情報３５０を携帯端末１０のメモリ３０に格納して登録する。

携帯端末１０を使用する際に、近傍にあるレッドバッジ７０の識別情報３

５０を確認する動作について、図２１のフローチャートを用いて説明する。図２１のフローチャートで説明するデフォルトモード１は、操作を開始しレッドバッジ７０の識別情報３５０が読み込まれたときに解除されるもので、通常操作を行っていない状態とする。また、デフォルトモード２は、いたずらされている可能性があるため、解除には暗証番号やバイオメトリックスなどを入力して本人である確認をする必要がある状態として以下説明する。

まず、携帯端末１０を使用する者がキー入力などの携帯端末１０を使用するための初動作を行った時点で、制御部４０のＣＰＵには割り込みが発生する（Ｓ１５０）。割り込みが発生すると、読み取り開始のコマンドを制御部４０から通信制御用ＩＣ２１に送られる。通信制御用ＩＣ２１は、読み取り開始のコマンドを受け取るとアンテナ２２から発信要求を発信して読み取りを開始する。

ここで、制御部４０はタイマーに所定の時間ｔ１を設定し（Ｓ１５１）、レッドバッジ７０から発信した識別情報３５０を受信したかチェックする（Ｓ１５２）。時間ｔ１が経過するまで識別情報３５０の受信したかを繰り返しチェックする（Ｓ１５３）。　時間ｔ１が経過しても、レッドバッジ７０から識別情報３５０の受信が完了しない場合は、デフォルトモード１を設定する（Ｓ１６２）。

識別情報３５０の受信が完了した場合は、受信した識別情報がメモリ３０に予め登録されている識別情報と比較し、該当するものがある場合には、登録済みのレッドバッジ７０が近くにあるので携帯端末１０の利用が可能である（Ｓ１５４）。該当するものがない場合には、登録済みのレッドバッジ７０ではない。そこで、登録されてない識別情報の受信回数が指定の回数より少ない場合は、デフォルトモード１を設定する（Ｓ１６２）が、登録されてない識別情報の受信回数が指定の回数より多い場合は、デフォルトモード２を設定する（Ｓ１６３）。

登録されている識別情報を受信した場合には（Ｓ１５４）、さらに、所定の時間ｔ２をタイマーに設定する（Ｓ１５６）。時間ｔ２が経過するまでに（Ｓ１５８）、通話・メール受信・インターネットのアクセスなどの処理を

開始しなかった場合は（Ｓ２０７）、デフォルトモード１を設定する（Ｓ１６２）。

時間ｔ２が経過するまでに（Ｓ１５８）、開始した通話・メール受信・インターネットのアクセスなどの処理が終了した場合は（Ｓ１５７）、所定の時間ｔ３をタイマーに設定する（Ｓ１５９）。時間ｔ３が経過するまでに（Ｓ１６１）、通話・メール受信・インターネットのアクセスなどの次の処理を開始した場合には（Ｓ１６０）、レッドバッジ７０の読み込みをすることはなく、引き続き作業を行うことができる。一つの作業が終了するたびにｔ３が起動され（Ｓ１５９）、ｔ３以内に次の作業が開始されないときは（Ｓ１６１）、デフォルトモード１になる（Ｓ１６２）。

図２１のフローチャートでは、携帯端末１０を利用する初動作に伴って発生した割り込み処理で、近傍にあるレッドバッジ７０の識別情報を確認する処理について説明したが、携帯端末１０を使用する際に、この割り込みの処理と同時に使用者の操作に応じた処理が平行して実行される。

また、デフォルトモード２の場合には、機能を停止し予め設定した動作をする。例えば、着信音を最大にして警告を発する。或いは、ダイヤルロックにすることも可能である。

デフォルトモードは各携帯端末１０の出荷時に設定されているが、購入後それぞれに応じた動作を使用者が任意に設定することができる。また、セキュリティレベルに応じて、携帯端末１０を利用する前には暗証番号を必ず入力しなければ使用できないようにするなど、使用者で変更可能である。

また、識別情報３５０の受信は、操作時の割り込み処理を使った例について説明したが、携帯端末１０からポーリングをしてレッドバッジ７０から識別情報３５０を受信し、定期的にレッドバッジ３の有り無しを確認することも可能である。

さらに、図２２に示す使用者識別システム１２’のように、第２の実施の形態で説明したように、携帯端末１０に定期券・乗車券・クレジットカード・鍵などの機能を内蔵させ、その機能を受信装置６０で受け取る場合に、まず、携帯端末１０の使用者が正当な使用者かをレッドバッジ７０で確認を取る

ようにすることも可能である。

以上、説明したようにレッドバッジに組み込んだ携帯記録素子の識別情報を確認して携帯端末１０の使用を可能にすることができ、正当な使用者にのみ使用を許可することができる。

第４の実施の形態では、携帯端末１０でＩＣチップなどの記録素子にデータを書き込む機能に付いて説明する。前述の実施の形態と同一のものには同一符号を付して詳細な説明を省略する。

第４の実施の形態における携帯記録素子書込システム１３は、図２３に示すように、携帯端末１０と記録素子５１とアンテナ２２を組み込んだＩＣカード５０とで概略構成される。ここでは、記録素子５１とアンテナ２２を組み込んだＩＣカード５０にデータを書き込む場合を例に説明する。

記録素子５１は、識別情報３５０を記録しているものである。

次に、本実施の形態の動作を図２４のフローチャートに従って説明する。

まず、携帯端末１０で書き込みモードの選択をした時点で、制御部４０のＣＰＵには割り込みが発生する（Ｓ１７０）。割り込みが発生すると、読み取り開始のコマンドを制御部４０から通信制御用ＩＣ２１に送られる。通信制御用ＩＣ２１では読み取り開始のコマンドを受け取るとアンテナ２２から読み取り要求（パワーパルスなど）を発信してＩＣカード５０に登録されている識別情報３５０の読み取りを開始する。

ここで、携帯端末１０の制御部４０はタイマーに所定の時間ｔ１を設定し（Ｓ１７１）、ＩＣカード５０から発信した識別情報３５０を受信したかチェックする（Ｓ１７２）。時間ｔ１が経過するまで識別情報３５０の受信を繰り返しチェックを行い（Ｓ１７３）、時間ｔ１が経過しても、ＩＣカード５０から識別情報３５０の受信が完了しない場合は、カードの認識不能の表示を行う（Ｓ１８０）。

識別情報３５０の受信が完了した場合は、受信した識別情報がメモリ３０に予め登録されている識別情報と比較して、該当するものがある場合には（Ｓ１７４）、登録済みのＩＣカード５０であるとする。該当するものがない場合には（Ｓ１７４）、登録済みのＩＣカード５０ではないので書込不可

の表示をする（Ｓ１８１）。

登録済みのＩＣカード５０の場合は、まず、書込カウンターＣを設定する（Ｓ１７５）。書込処理（Ｓ１７６）を行い正常に書込処理が終了しない場合は（Ｓ１７７）、書込カウンターＣが０になるまで（Ｓ１７８）、再度書込処理（Ｓ１７６）をする。書込カウンターＣが０になっても書き込みができない場合は書込不良を表示する（Ｓ１８２）。

正常に書き込みが終了すると書込終了を表示する（Ｓ１７９）。

以上、説明したように、ＲＦＩＤインターフェースを備えた携帯端末１０では、受信したデジタルチケットなどのデジタル情報をＩＣカード５０に書き込むことが可能である。また、携帯端末１０を利用してインターネットなどの銀行からキャッシングしてＩＣカード５０に書き込むことも可能である。

さらに、図２５に示す携帯記録素子書込システム１３’のように、ＩＣカード５０に書き込みを行う際、第３の実施の形態で説明したように携帯端末１０の使用者が正当な使用者かをレッドバッジ７０で確認を取るようにすることも可能である。

これにより、正当な携帯端末１０の利用者のみＩＣカード５０に書き込みが行える。

第５の実施の形態では、インターネットなどの回線を利用して携帯端末１０やＩＣカード５０の利用状況を管理する第１の利用管理システムについて説明する。前述の実施の形態と同一のものには同一符号を伏して詳細な説明を省略する。

第５の実施の形態における利用管理システム１４は、図２６に示すように、携帯端末１０やＩＣカード５０などの記録素子とＲＦＩＤインターフェースの送受信部を組み込んだ装置９０と管理サーバ１００とが通信回線１１０を介して接続される。さらに、通信回線１１０には、銀行の端末やネットバンクなどの金融機関１２０が接続される構成になっても良い。

この携帯端末１０やＩＣカード５０などの記録素子には、各個体が一意に識別できる識別情報３５０が書換不可能に記録されている。また、携帯端末

１０には、ＲＦＩＤインターフェースの送受信部２０を備え、識別情報３５０を発信する機能を備える。さらに、携帯端末１０には、通信回線送信部２５を備え、通信回線を介してインターネットなどに接続する機能を備えている。

ここでは、装置９０は、自動販売機にＲＦＩＤインターフェースの送受信部を組み込んだものを例に説明する。装置９０より、ＲＦＩＤインターフェースを備える携帯端末１０やＩＣカード５０などと送受信することが可能で、代金を携帯端末１０やＩＣカード５０に記録されているプリペイドカードやキャッシュカードなどから代金を受領する機能を備えている。

また、装置９０には、管理サーバ１００と通信回線１１０を介して送受信を行うサーバ接続部８０を備える。さらに、装置９０には、装置毎に割り振られる装置番号９１を記録している。

管理サーバ１００は、携帯端末１０やＩＣカード５０の識別情報３５０とその利用情報とをともに通信回線１１０を介して受信し、利用内容を表す利用情報を管理する管理部を備える。

通信回線１１０は、専用回線やインターネットなどである。情報管理の信頼性の観点から、セキュリティの確保されているものが好ましい。

次に、本実施の形態の動作を携帯端末１０を例に、図２７のフローチャートと図２８の携帯端末１０の画面の遷移図に従って説明する。

まず、携帯端末１０では、図２８の画面の遷移図に示すように、メニューからプリペイドカードのモード１０００～商品購入モード１００１～自動販売機モード１００２を選択する（Ｓ３００）。ここで、識別情報３５０を携帯端末１０のＲＦＩＤインターフェースから自動販売機９０に発信すると、携帯端末１０には、個人認証中の画面１００３が表示される（Ｓ３０１）。以下、自動販売機９０と携帯端末１０とは、ＲＦＩＤインターフェースで送受信されるものとする。

自動販売機９０では、識別情報３５０を受け取ると、携帯端末１０の識別情報３５０と自動販売機９０の装置番号９１とを管理サーバ１００にサーバ接続部８０から送信して、残高確認及びブラックリストとの照合を行う

（Ｓ４００）。管理サーバ１００では、識別番号３５０から携帯端末１０の所有者の個人データをチェックする。さらに、ブラックリストのチェックを行う（Ｓ５００）。

あるいは、一度受信したブラックリストを自動販売機９０に記憶しておき、自動販売機９０でチェックを行うようにすることも可能である。これにより、管理サーバ１００との送受信の時間に要する時間を短縮し、利便性を高めることも可能である。

以下、自動販売機９０と管理サーバ１００とは、サーバ接続部８０から送受信されるものとする。

自動販売機９０では、管理サーバ１００でのチェック結果より個人データ及びブラックリストに問題がある場合は（Ｓ４００）、携帯端末１０に購入不可を発信する。携帯端末１０には使用不能を表す画面１００７を表示する（Ｓ３０２）。

また、個人データ及びブラックリストに問題が無ければ（Ｓ４００）、携帯端末１０に購入許可を発信する。携帯端末１０には商品の選択画面１００４を表示する（Ｓ３０３）。

自動販売機９０で商品を選択すると（Ｓ４０１）、自動販売機９０から携帯端末１０に商品代金の引き落としデータが送られる（Ｓ４０２）。携帯端末１０では、代金減算処理が行われ、処理中の画面１００５が表示される（Ｓ３０４）。さらに、このとき携帯端末１０から代金引き落としの処理が正常に行われなかった場合には（Ｓ４０２）、利用情報としてＮＧの通知が自動販売機９０から管理サーバ１００に送信され、個人データまたはブラックリストが更新される（Ｓ５０１）。

自動販売機９０では、携帯端末１０から代金引き落としの処理が正常に行われたが（Ｓ４０２）、商品の払い出しが正常に行われなかった場合には（Ｓ４０３）、利用情報としてＮＧの通知を自動販売機９０から管理サーバ１００に送信され、正常に動作しなかった自動販売機９０の装置番号９１が記録される（Ｓ５０２）。

また、携帯端末１０から代金引き落としの処理が正常に行われ（Ｓ４０２）、

さらに、商品の払い出しが正常に行われた場合には（Ｓ４０３）、購入処理完了を自動販売機９０から携帯端末１０に発信する。携帯端末１０では残金が画面１００６に表示される。（Ｓ３０５）。さらに、利用情報として購入情報が自動販売機９０から管理サーバ１００に送信され、履歴として記録される（Ｓ５０３）。

ここでは、携帯端末１０について説明したがＩＣカード５０でも同様に行うことができる。

また、自動販売機９０から商品が正常に払い出しされなかった場合には、携帯端末１０の通信回線送信部２５より通信回線１１０を介して管理サーバ１００に接続して、携帯端末１０の識別番号３５０と自動販売機９０を利用した利用情報とをもとに、装置番号９１よりどの自動販売機９０を利用したかが確認でき、代金の払い戻しを受けることも可能である。

さらに、自動販売機９０の装置番号９１を携帯端末１０のＲＦＩＤインターフェースの送受信部２０を介して受信し、利用情報と携帯端末１０の識別情報３５０と装置番号９１とを、携帯端末１０の通信回線送信部２５より通信回線１１０を介して管理サーバ１００に送信することも可能である。

ここでは、携帯端末１０をプリペイドカードとして利用した場合について説明したが、携帯端末１０をキャッシュカード・デビットカード・ポイントカード・スマートカードクレジットカードなどとして利用した場合でも同様に行える。

また、ここでは情報はセキュリティ上、暗号化されて管理サーバに送信されることが好ましい。

以上、説明したように、携帯端末１０に一意に割り振られる識別情報３５０と利用情報を関連付けて管理することにより携帯端末１０の利用履歴をとることができる。

携帯端末１０にＧＰＳ（Global Positioning System）機能を備え、位置情報を取得して携帯端末１０の位置を正確に把握することにより、装置番号９１とを比較することで不正利用を防ぐことが可能である。

さらに、図２９に示す利用管理システム１４’のように、携帯端末１０を

使用する際、第３の実施の形態で説明したように携帯端末１０の使用者が正当な使用者かをレッドバッジ７０で確認を取るようにすることも可能である。

これにより、正当な携帯端末１０の利用者のみ携帯端末１０を使用することができる。

第６の実施の形態では、インターネットなどの回線を利用して携帯端末１０やＩＣカード５０にキャッシュカードやプリペイドカードの機能を登録する第２の利用管理システムについて説明する。前述の実施の形態と同一のものには同一符号を伏して詳細な説明を省略する。

第６の実施の形態における利用管理システム１５は、図３０に示すように、携帯端末１０やＩＣカード５０とＲＦＩＤインターフェースの送受信部２０を組み込んだ装置９０'と管理サーバ１００とが通信回線１１０を介して接続される。さらに、通信回線１１０には、銀行の端末やネットバンクなどの金融機関１２０が接続される。

装置９０'は、ＲＦＩＤインターフェースの送受信部２０を備えたプリペイド購入機９０'とし、携帯端末１０やＩＣカード５０に対して、プリペイドカードの残高の書換が行われるものを例に説明する。さらに、装置９０'には、装置毎に割り振られる装置番号９１を記録している。

次に、本実施の形態の動作を図３１のフローチャートと図３２の携帯端末１０の画面の遷移図に従って説明する。

まず、携帯端末１０では、図３２の画面の遷移図に示すように、メニューからプリペイドカードのモード１１００～現金加算モード１１０１を選択する（Ｓ３１０）。ここで、識別情報３５０をＲＦＩＤインターフェースで携帯端末１０からプリペイド購入機９０'に発信すると、携帯端末１０には、個人認証中の画面１１０２が表示される（Ｓ３１１）。

プリペイド購入機９０'では、識別情報３５０を受け取ると、携帯端末１０の識別情報３５０をサーバ接続部８０から管理サーバ１００に送信して、残高確認及びブラックリストとの照合を行う（Ｓ４１０）。管理サーバ１００では、識別番号３５０から携帯端末１０の所有者の個人データをチェック

する。さらに、ブラックリストのチェックを行う（Ｓ５１０）。以下、プリペイド購入機９０’と管理サーバ１００とは、サーバ接続部８０から送受信されるものとする。

プリペイド購入機９０’では、個人データ及びブラックリストに問題がある場合は（Ｓ４１０）、携帯端末１０に加算不可を発信する。携帯端末１０では加算不能を表す画面１１０６を表示する（Ｓ３１２）。

また、個人データあるいはブラックリストに問題が無ければ（Ｓ４１０）、携帯端末１０に購入許可を発信する。携帯端末１０には加算金額の選択画面１１０３を表示する（Ｓ３１３）。プリペイド購入機９０’では、加算金額が選択される（Ｓ４１１）と携帯端末１０に加算金額のデータを送る（Ｓ４１２）。

ここで、指定された金額が金融機関１２０に残高があるかを確認し（Ｓ４１２）、不足の場合は、携帯端末１０に残金不足を発信して残金不足のエラー画面１１０７を表示する（Ｓ３１４）。不足に問題がない場合は、加算処理が行われ、処理中の画面１１０４が表示される（Ｓ３１５）。さらに、このとき携帯端末１０から加算処理が正常に行われなかった場合には（Ｓ４１３）、利用情報としてＮＧの通知が管理サーバ１００に送信され、個人データにエラーが記録される（Ｓ５１１）。さらに、携帯端末１０には加算処理異常のエラー画面１００８が表示される（Ｓ３１６）。

携帯端末１０から加算処理が正常に行われた場合には（Ｓ４１３）、残高が携帯端末１０の画面１１０８に表示され（Ｓ３１７）、利用情報として加算情報とプリペイド購入機９０’の装置番号９１とが管理サーバ１００に送信され履歴として記録される（Ｓ５１２）。

また、銀行などの金融機関１２０から引き落として携帯端末１０に加算処理をする例について説明したが、プリペイド購入機９０’に現金を投入して携帯端末１０に加算処理をすることも可能である。

さらに、自動販売機９０をプリペイドカード購入機９０’として利用することも可能である。

ここでは、携帯端末１０をプリペイドカードとして利用した場合について

説明したが、キャッシュカード・デビットカード・クレジットカード・会員権・診察券・健康保健所・身分証明書・アミューズメント施設のチケット類などでも同様におこなうことが可能である。

また、本実施の形態では、ＲＦＩＤインターフェースをもつ専用機９０'を例に説明したが、金融機関１２０から通信回線１１０を介して直接引き落として携帯端末１０に加算処理をし、さらに、管理サーバ１００へ携帯端末１０の識別情報３５０と利用情報と送信するようにすることもできる。

各種クレジット会社との通信回線１１０を介して送受信することにより、クレジットカードの機能を携帯端末１０に追加することも可能である。

以上、説明したように、携帯端末１０にカードなどの機能を持たせることができ、さらに、識別番号３５０から携帯端末１０に登録されている全ての利用状況を管理することができる。

さらに、図３３に示す利用管理システム１５'のように、携帯端末１０に加算処理をする際に、第３の実施の形態で説明したように携帯端末１０の使用者が正当な使用者かをレッドバッジ７０で確認を取るようにすることも可能である。

これにより、正当な携帯端末１０の利用者のみ携帯端末１０に加算処理をすることができる。

第７の実施の形態では、ＲＦＩＤインターフェースを持つ携帯端末１０同士の送受信について説明する。前述の実施の形態と同一のものには同一符号を伏して詳細な説明を省略する。

図３４に示すように、携帯端末１０と携帯端末１０とを近づけることによりＲＦＩＤインターフェースを使用して送受信を行うことが可能である。例えば、デジタルマネー・着メロ・待ち受け画面などのデジタル情報を相手側の携帯端末１０に渡すことが可能である。

以上詳細に説明したように、本発明では、携帯端末に定期券・クレジットカード・運転免許書などの個人情報を携帯端末に登録することができる。

また、携帯端末に一意に割り振られる識別情報をもとに携帯端末の利用状況の履歴を取ることが確実に行われ悪用を防ぐことができる。

さらに、携帯端末が悪意を持つ第３者に渡っても、対応するレッドバッジ（ＩＣチップ）などがない限り悪用できない。

また、これにより、利用した覚えのない料金を支払う必要がない。

或いは、携帯端末に記憶されている個人データの流出を防ぐことが可能になる。

また、非接触ＩＣチップとも送受信ができ、携帯端末からＩＣカードの識別を行うこともできる。さらに、書き込みが行え、容易にＲＦＩＤシステムが構築できる。

請求の範囲

1. 被保護情報が記録された第１アセンブリと、認証情報が記録された第２アセンブリとを含む情報保護システムであって、

前記第２アセンブリは前記第１アセンブリからの要求に応じて非接触による情報の送信を可能にする通信手段を備えるものであり、

前記第１アセンブリは、

前記被保護情報に対するアクセスを受け付ける受付手段と、

前記認証情報を前記第２アセンブリより受け取って認証を行う認証手段と、

この認証手段による認証結果に応じて前記受付手段で受け付けたアクセスを許可又は禁止するアクセス制御手段とを備えるものである、

情報保護システム。

2. 認証用情報と被保護情報とが記録された第１アセンブリと、第２アセンブリとを含む情報保護システムであって、

前記第１アセンブリ及び前記第２アセンブリは、それぞれ、他方のアセンブリとの間で非接触による情報の送受信を可能にする通信手段を備えるものであり、

前記第２アセンブリは、さらに、前記認証情報を前記第１アセンブリより受け取って認証を行う認証手段を備え、

前記第１アセンブリは、さらに、

前記被保護情報に対するアクセスを受け付ける受付手段と、

前記第２アセンブリから前記認証手段による認証結果を受信するとともにその認証結果に応じて前記受付手段で受け付けたアクセスを許可又は禁止するアクセス制御手段とを備えるものである、

情報保護システム。

3. その所有者を認証するための第１認証情報と被保護情報とが記録された第１アセンブリと、前記所有者を認証するための第２認証情報が記録された第２アセンブリとを含む情報保護システムであって、

前記第１アセンブリ及び前記第２アセンブリは、それぞれ、他方のアセンブリとの間で非接触による情報の送受信を可能にする通信手段を備えるものであり、

前記第２アセンブリは、さらに、第１認証情報を前記第１アセンブリより受け取り、受け取った第１認証情報と前記第２認証情報とに基づく認証を行う第２認証手段を備え、

前記第１アセンブリは、さらに、

前記被保護情報に対するアクセスを受け付ける受付手段と、

前記第２認証情報を前記第２アセンブリより受け取り、受け取った第２認証情報および前記第１認証情報とに基づく認証を行う第１認証手段と、

前記第１認証手段による認証結果および前記第２アセンブリより受け取った前記第２認証手段による認証結果に応じて前記受付手段で受け付けたアクセスを許可又は禁止するアクセス制御手段とを備えるものである、

情報保護システム。

4．前記第１アセンブリ、第２アセンブリは、いずれも、単独で携帯可能であるか、または携帯可能な製品に内蔵されていることを特徴とする、

請求項１記載の情報保護システム。

5．前記第１アセンブリ、第２アセンブリは、いずれも、単独で携帯可能であるか、または携帯可能な製品に内蔵されていることを特徴とする、

請求項２記載の情報保護システム。

6．前記第１アセンブリ、第２アセンブリは、いずれも、単独で携帯可能であるか、または携帯可能な製品に内蔵されていることを特徴とする、

請求項３記載の情報保護システム。

7．前記通信手段が、電磁誘導による無線通信、電磁結合による無線通信、静電結合による無線通信、及び光を情報の搬送媒体とする通信、のいずれかを行う、

請求項１記載の情報保護システム。

8．前記被保護情報が個人のプライバシーに関わる情報及び/または財的価値に関わる情報である、

請求項１記載の情報保護システム。

9. 前記第１アセンブリおよび前記第２アセンブリが、それぞれ非接触通信用のアンテナを含むＩＣモジュールである、

請求項１記載の情報保護システム。

10. 前記第１アセンブリがカード媒体に埋め込まれたものである、

請求項１記載の情報保護システム。

11. 前記第１アセンブリがシート状の媒体に埋め込まれたものである、

請求項１記載の情報保護システム。

12. 前記第１アセンブリが携帯性端末に内蔵されたものである、

請求項１記載の情報保護システム。

13. 前記第１アセンブリがデータキャリアに内蔵されたものである、

請求項１記載の情報保護システム。

14. 前記第２アセンブリが前記第１アセンブリを所持する者が身につける装飾品に埋め込まれたものである、

請求項１記載の情報保護システム。

15. その所有者を認証するための第１認証情報と被保護情報とが記録された第１アセンブリと、前記所有者を認証するための第２認証情報が記録された第２アセンブリと、前記被保護情報を読み取る情報読取装置とを含む情報保護システムであって、

前記第１アセンブリは、前記第２アセンブリおよび情報読取装置との間で非接触による情報の送受信を可能にする第１通信手段を備えるものであり、

前記第２アセンブリは、前記１アセンブリとの間で非接触による情報の送受信を可能にする第２通信手段を備えるものであり、

前記情報読取装置は、前記第１アセンブリとの間で非接触による情報の送受信を可能にする第３通信手段を備えるものであり、

前記第１アセンブリは、さらに、前記情報読取装置からの信号に応答して前記第２アセンブリより前記第２認証情報を受け取り、受け取った第２認証情報および前記第１認証情報に基づく認証を行い、認証結果に応じて前記被保護情報の前記情報読取装置による読み取りを許可又は禁止する手段を備

えるものである、

情報保護システム。

16. その所有者を認証するための第１認証情報と被保護情報とが記録された第１アセンブリと、前記所有者を認証するための第２認証情報が記録された第２アセンブリと、前記被保護情報を読み取る情報読取装置とを含む情報保護システムであって、

前記第１アセンブリは、前記第２アセンブリおよび情報読取装置との間で非接触による情報の送受信を可能にする第１通信手段を備えるものであり、

前記第２アセンブリは、前記１アセンブリとの間で非接触による情報の送受信を可能にする第２通信手段を備えるものであり、

前記情報読取装置は、前記第１アセンブリとの間で非接触による情報の送受信を可能にする第３通信手段を備えるものであり、

前記第２アセンブリは、さらに、前記第１認証情報を前記第１アセンブリより受け取るとともに受け取った第１認証情報および前記第２認証情報に基づく認証を行い、認証結果を前記第１アセンブリに送信する手段を備え、

前記第１アセンブリは、さらに、前記情報読取装置からの信号に応答して前記第２アセンブリに前記第１認証情報を送信するとともに当該第２アセンブリから前記認証結果を受け取り、受け取った認証結果に応じて前記被保護情報の前記情報読取装置による読み取りを許可又は禁止する手段を備えるものである、

情報保護システム。

17. その所有者を認証するための第１認証情報と被保護情報とが記録された第１アセンブリと、前記所有者を認証するための第２認証情報が記録された第２アセンブリと、前記被保護情報を読み取る情報読取装置とを含む情報保護システムであって、

前記第１アセンブリは、前記第２アセンブリおよび情報読取装置との間で非接触による情報の送受信を可能にする第１通信手段を備えるものであり、

前記第２アセンブリは、前記１アセンブリとの間で非接触による情報の送受信を可能にする第２通信手段を備えるものであり、

前記情報読取装置は、前記第１アセンブリとの間で非接触による情報の送受信を可能にする第３通信手段を備えるものであり、

前記第２アセンブリは、さらに、第１認証情報を前記第１アセンブリより受け取り、受け取った第１認証情報および前記第２認証情報に基づく第２認証を行うとともに認証結果を前記第１アセンブリに送信する第２認証手段を備え、

前記第１アセンブリは、さらに、

前記情報読取装置からの信号に応答して前記第２アセンブリに前記第１認証情報を送信するとともに当該第２アセンブリから前記第２認証情報を受け取り、受け取った第２認証情報および前記第１認証情報とに基づく第１認証を行う第１認証手段と、

前記第１認証手段による認証結果および前記第２アセンブリより受け取った前記第２認証手段による認証結果に応じて前記被保護情報の前記情報読取装置による読み取りを許可又は禁止する手段を備えるものである、

情報保護システム。

18. 前記第１アセンブリ、第２アセンブリは、いずれも、単独で携帯可能であるか、または携帯可能な製品に内蔵されていることを特徴とする、

請求項１５記載の情報保護システム。

19. 前記第１アセンブリ、第２アセンブリは、いずれも、単独で携帯可能であるか、または携帯可能な製品に内蔵されていることを特徴とする、

請求項１６記載の情報保護システム。

20. 前記第１アセンブリ、第２アセンブリは、いずれも、単独で携帯可能であるか、または携帯可能な製品に内蔵されていることを特徴とする、

請求項１７記載の情報保護システム。

21. 前記第１乃至第３通信手段が、電磁誘導による無線通信、電磁結合による無線通信、静電結合による無線通信、及び光を情報の搬送媒体とする通信、のいずれかを行う、

請求項１５記載の情報保護システム。

22. 前記被保護情報が個人のプライバシーに関わる情報及び/または財的

価値に関わる情報である、請求項１５記載の情報保護システム。

23. 前記第１アセンブリおよび前記第２アセンブリが、それぞれ非接触通信用のアンテナを含むＩＣモジュールである、

請求項１５記載の情報保護システム。

24. 前記第１アセンブリがカード媒体に埋め込まれたものである、

請求項１５記載の情報保護システム。

25. 前記第１アセンブリがシート状の媒体に埋め込まれたものである、

請求項１５記載の情報保護システム。

26. 前記第１アセンブリが携帯性端末に内蔵されたものである、

請求項１５記載の情報保護システム。

27. 前記第２アセンブリが前記第１アセンブリを所持する者が身につける装飾品に埋め込まれたものである、

請求項１５記載の情報保護システム。

28. それぞれ異なる箇所で独立して存在し、互いの間で非接触による情報の送受信が可能な第１アセンブリおよび第２アセンブリのうち、第１アセンブリに被保護情報を記録しておき、

前記被保護情報へのアクセス要求があったときに、前記第１アセンブリとの間で非接触による通信が可能な領域に前記第２アセンブリが存在することを条件として、前記第１アセンブリが、前記アクセス要求を許可することを特徴とする、

情報保護方法。

29. 前記第１アセンブリと前記第２アセンブリは、いずれも携帯可能な製品に内蔵されていることを特徴とする、

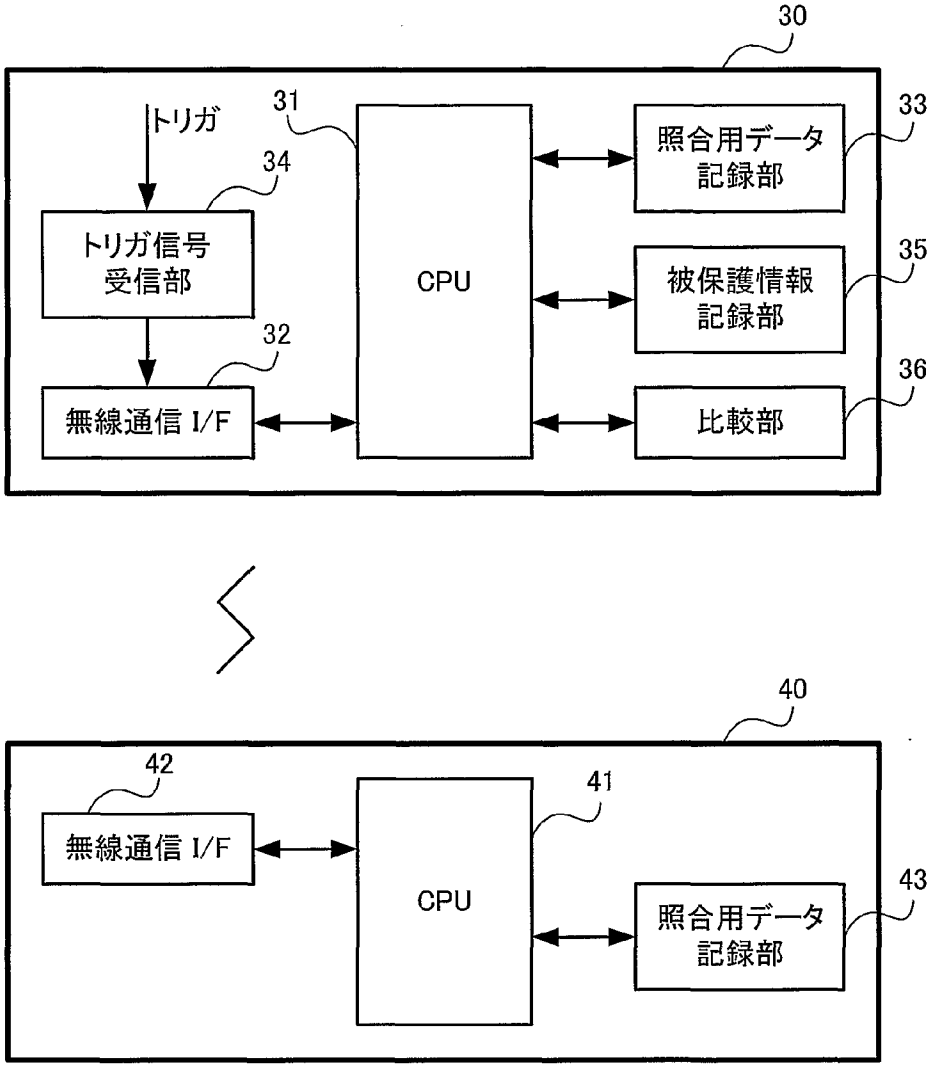
請求項２８記載の方法。

30. 前記第１アセンブリと前記第２アセンブリの少なくとも一方に、前記第１アセンブリの保有者を一意に識別するための認証情報を記録しておき、この認証情報に基づく認証の結果、前記保有者であることが確認された場合に、前記第１アセンブリが前記アクセス要求を許可することを特徴とする、

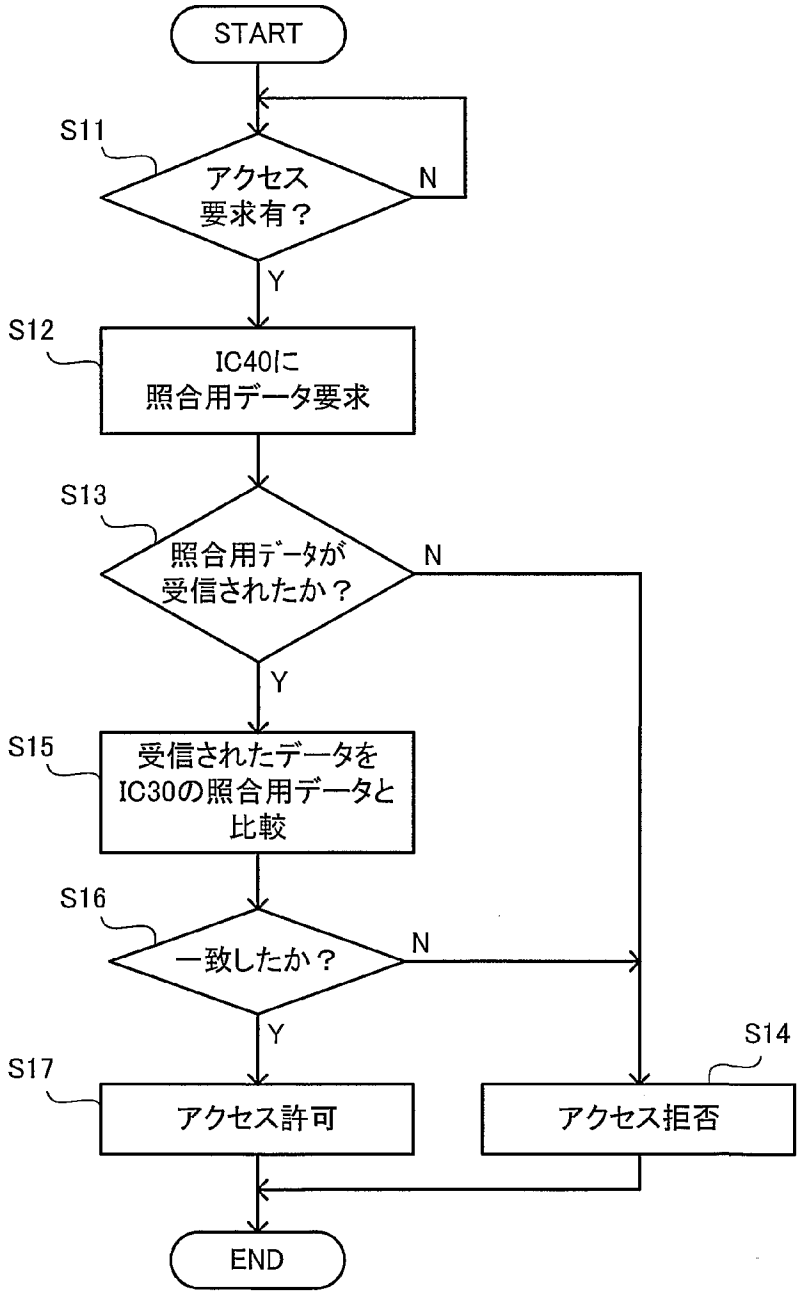
請求項２８記載の方法。

31. 前記アクセス制御手段は、当該認証手段でアクセスを許可するという認証結果が得られた場合は、前記アクセス要求から所定時間が経過するまでは、被保護情報へのアクセスを許可することを特徴とする、請求項１記載の情報保護システム。

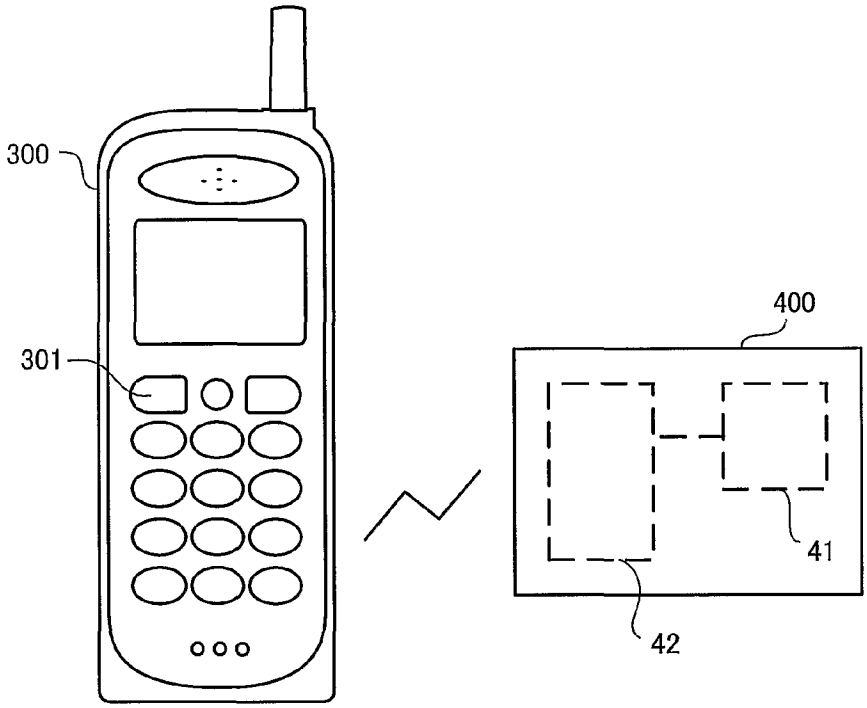
32. 前記アクセス制御手段は、当該認証手段でアクセスを許可するという認証結果が得られた場合は、前記アクセス要求から所定時間が経過するまでは、被保護情報へのアクセスを許可することを特徴とする、請求項１５記載の情報保護システム。


30
トリガ
31
33
34
照合用データ
記録部
トリガ信号
受信部
CPU
35
被保護情報
記録部
32
36
無線通信 I/F
比較部
40
42
41
無線通信 I/F
CPU
43
照合用データ
記録部

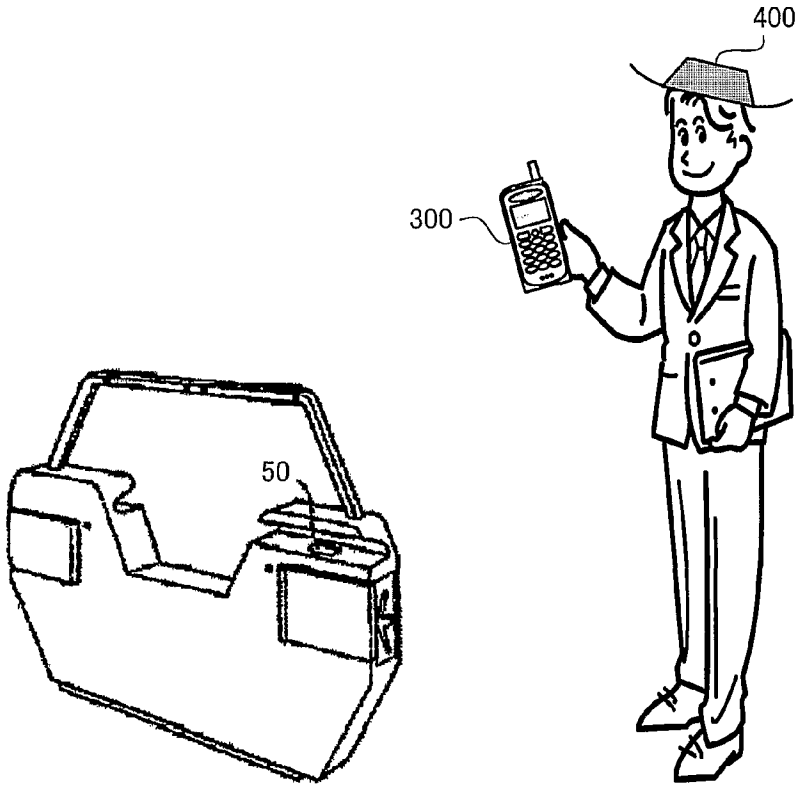
第1図


START
S11
アクセス
要求有？
N
Y
S12
IC40に
照合用データ要求
S13
照合用ﾃﾞｰﾀが
受信されたか？
N
Y
S15
受信されたデータを
IC30の照合用データと
比較
S16
一致したか？
N
Y
S14
S17
アクセス許可
アクセス拒否
END

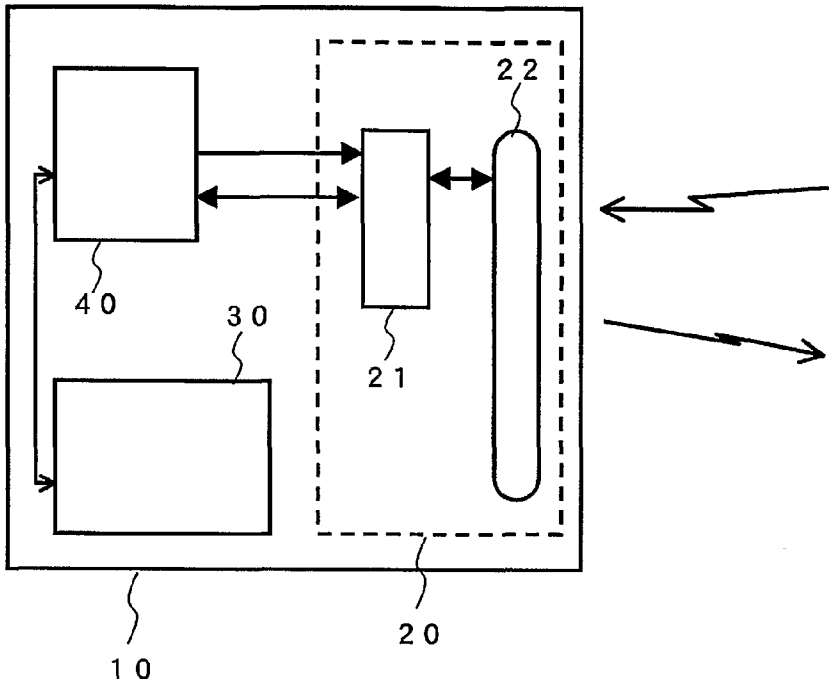
第2図



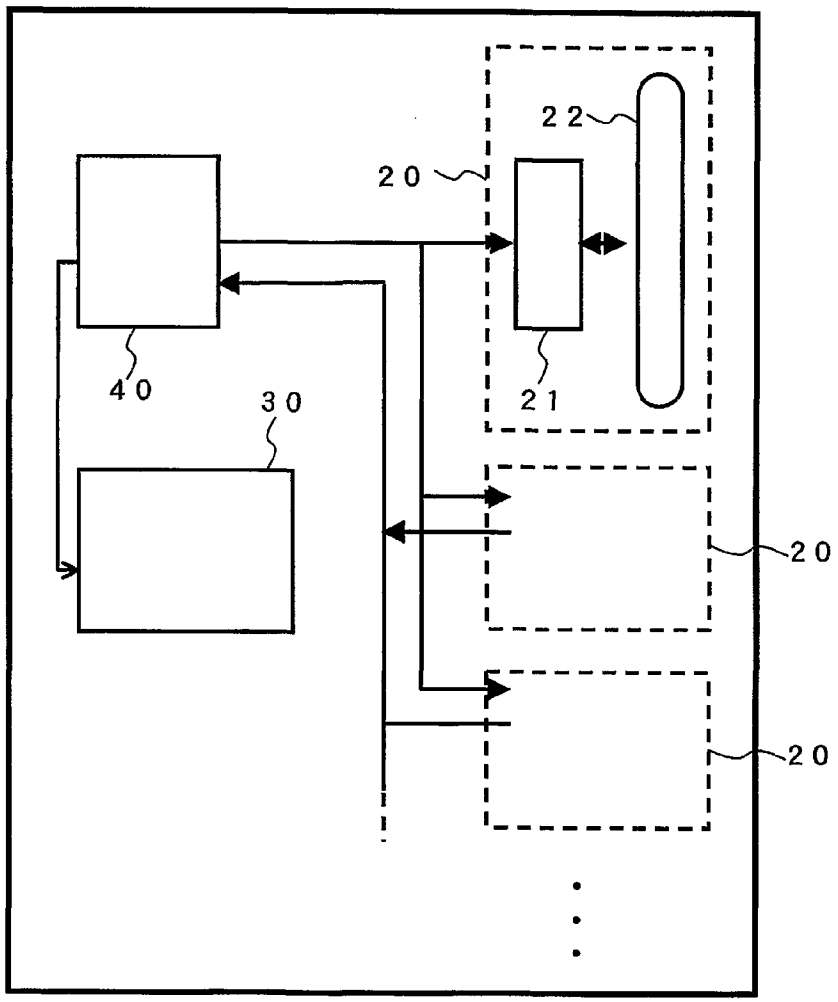
第3図



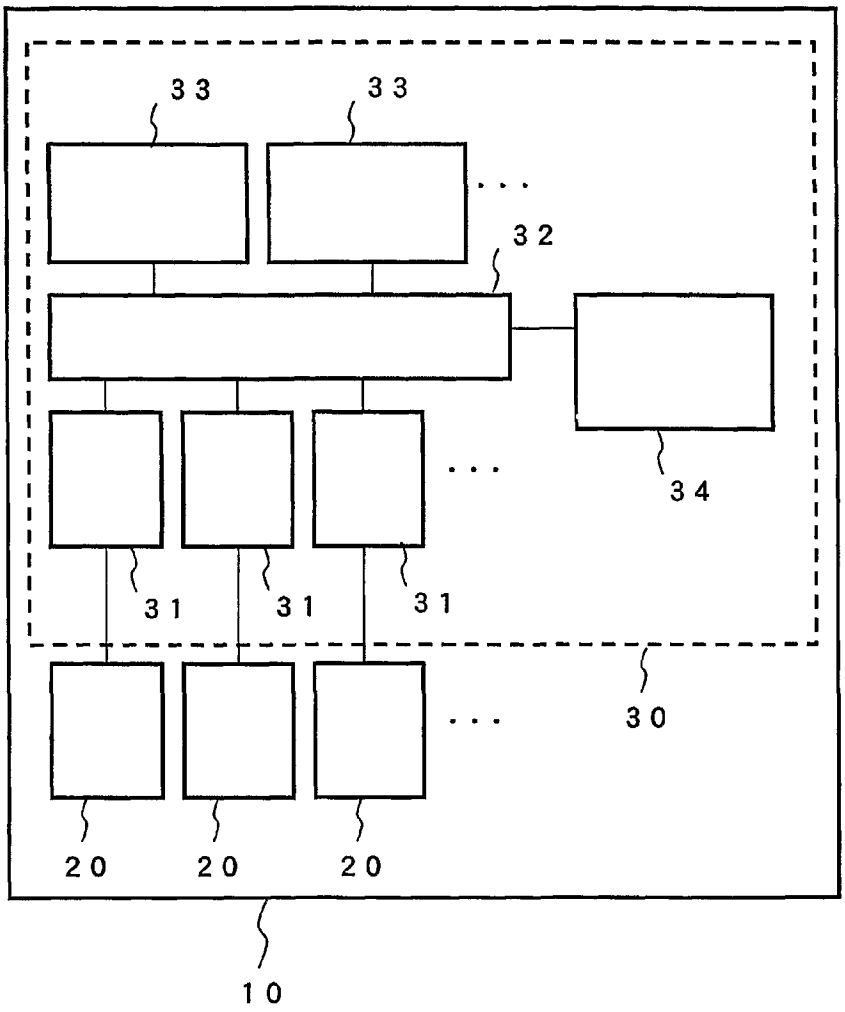
第4図



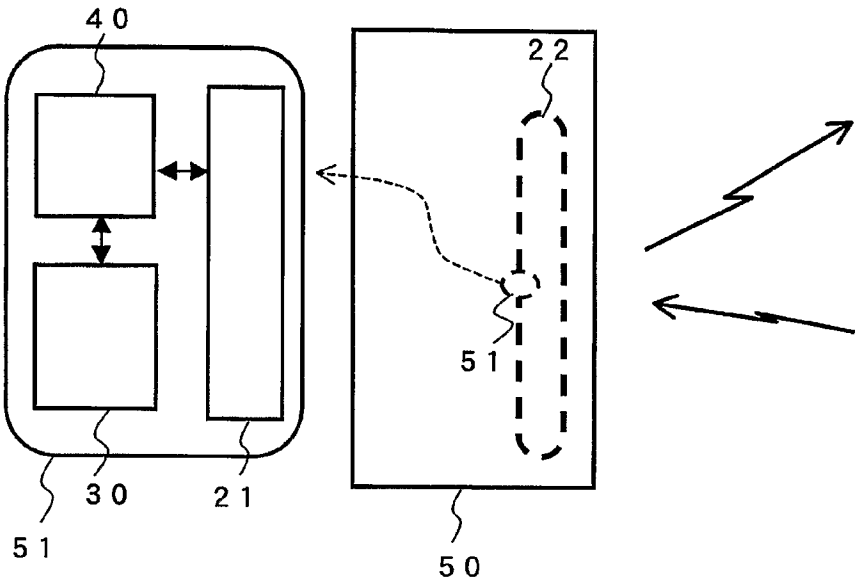
第5図



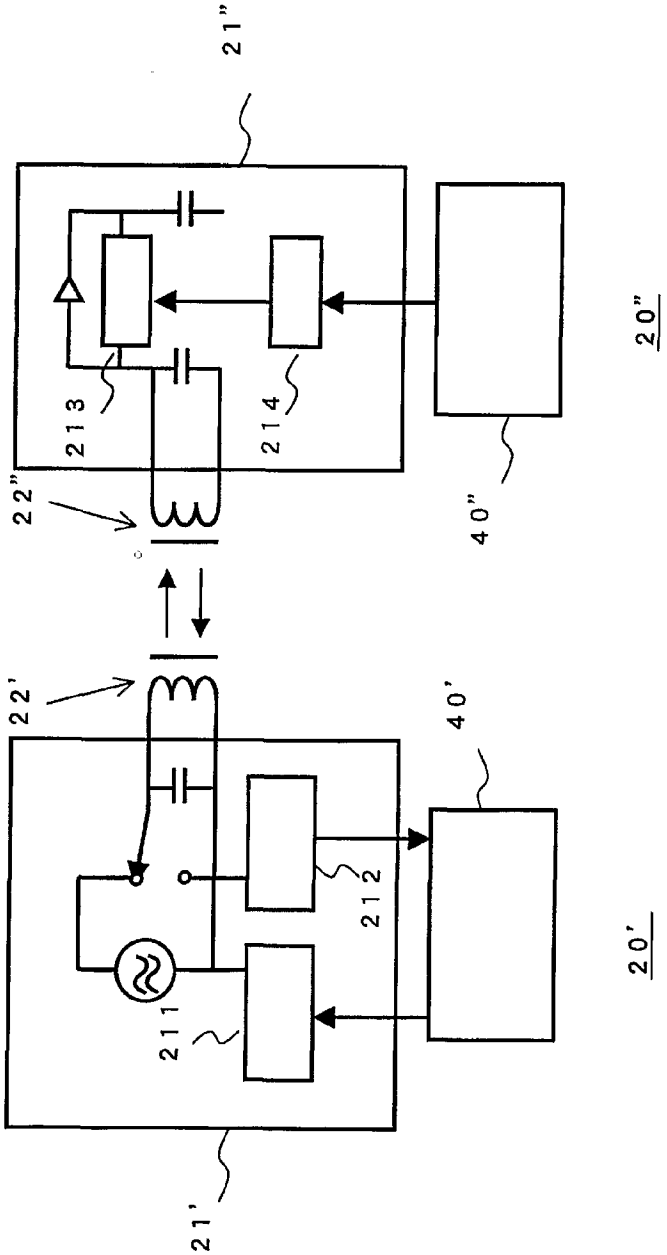
第6図



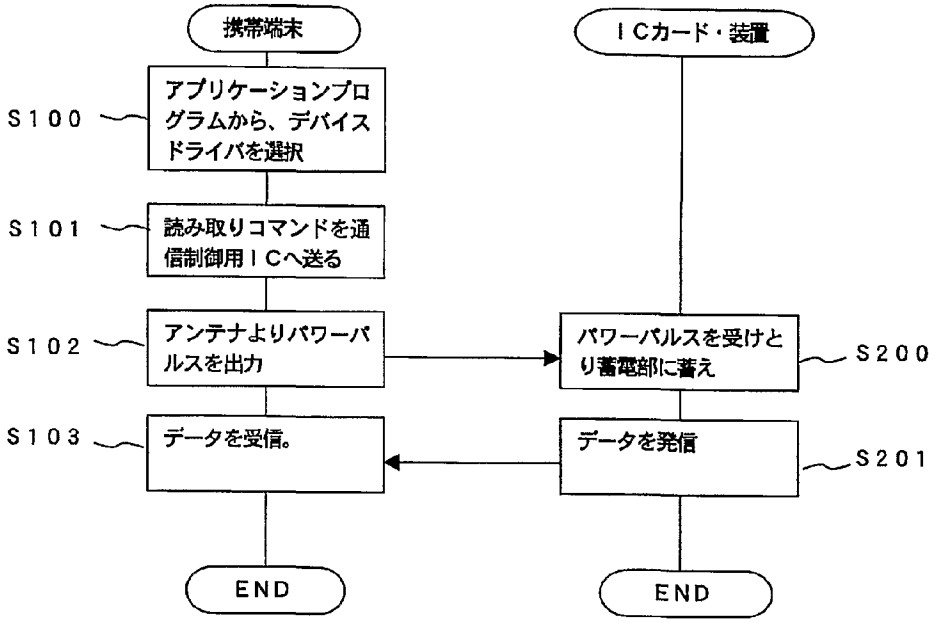
第7図



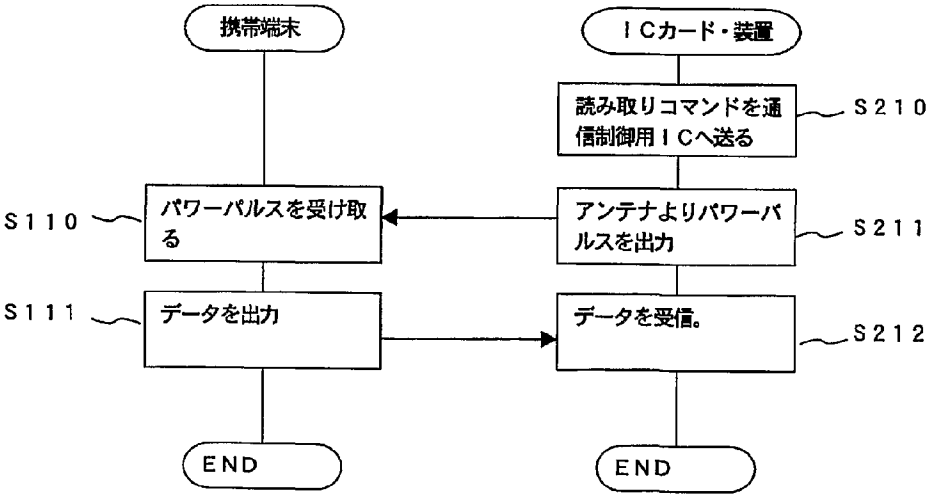
第8図



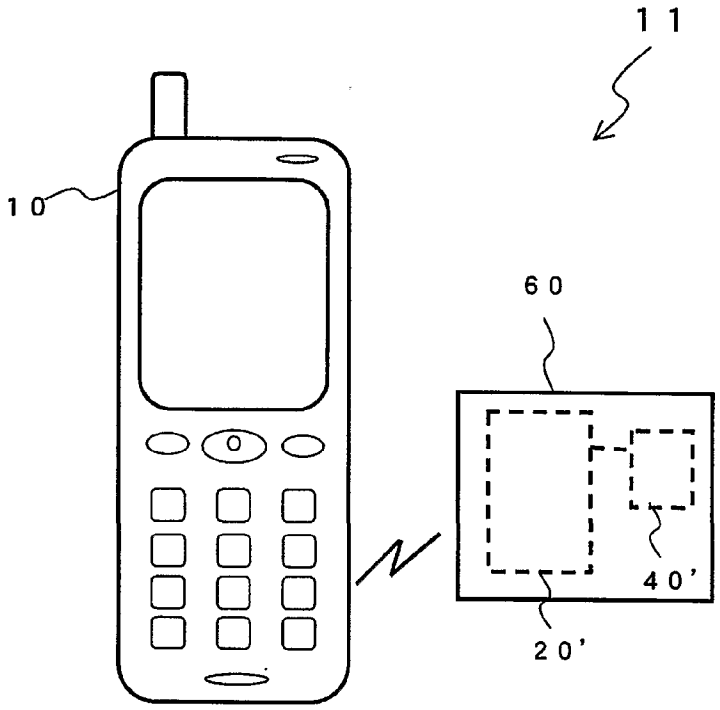
第9図


携帯端末
ＩＣカード・装置
アプリケーションプログラムから、デバイスドライバを選択
S100
読み取りコマンドを通信制御用ＩＣへ送る
S101
アンテナよりパワーパルスを出力
S102
パワーパルスを受けとり蓄電部に蓄え
S200
データを受信。
S103
データを発信
S201
END
END

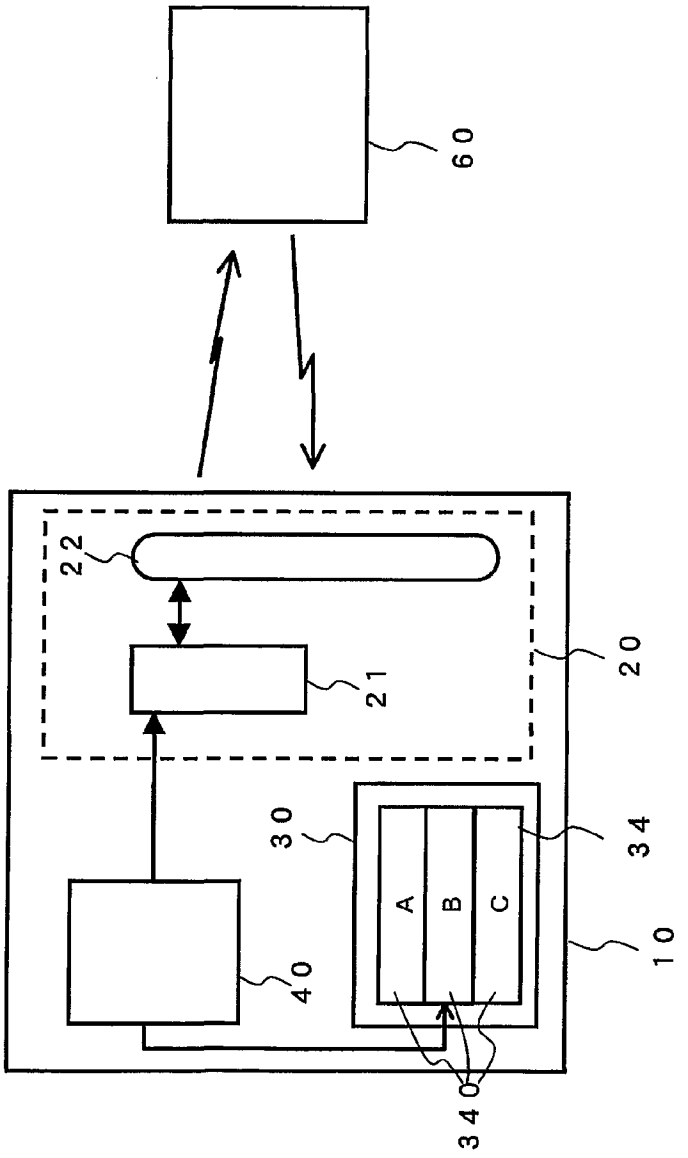
第10図


携帯端末
ＩＣカード・装置
読み取りコマンドを通信制御用ＩＣへ送る
S210
パワーパルスを受け取る
S110
アンテナよりパワーパルスを出力
S211
データを出力
S111
データを受信。
S212
END
END

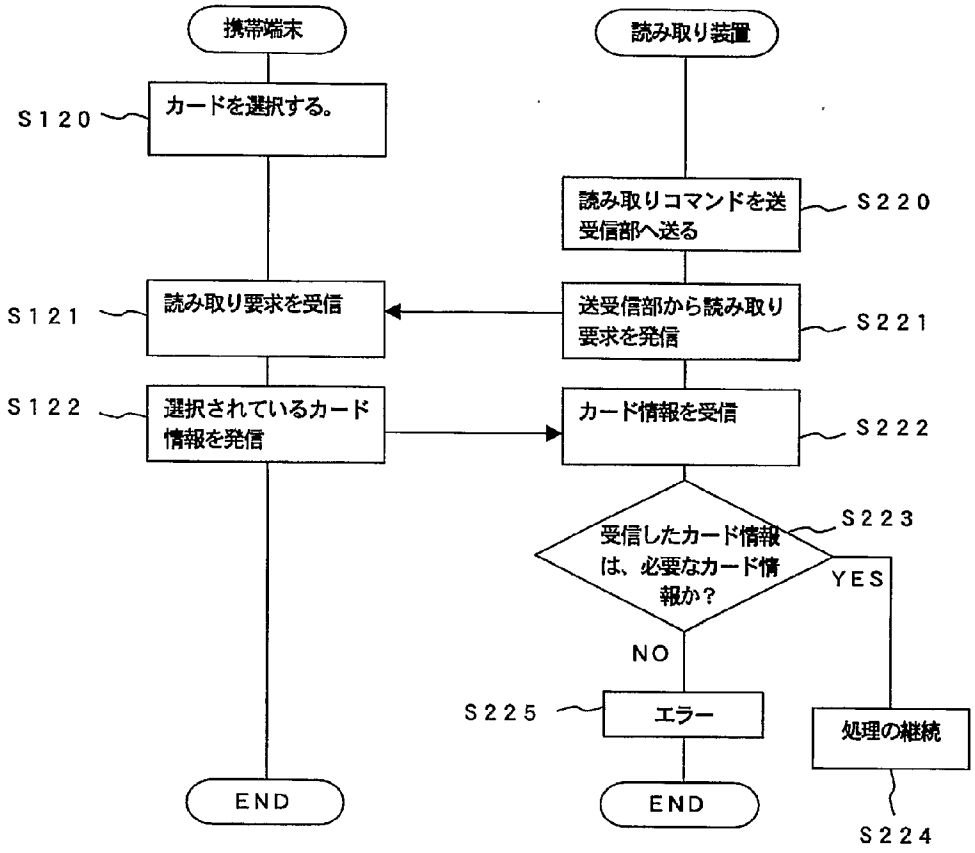
第11図



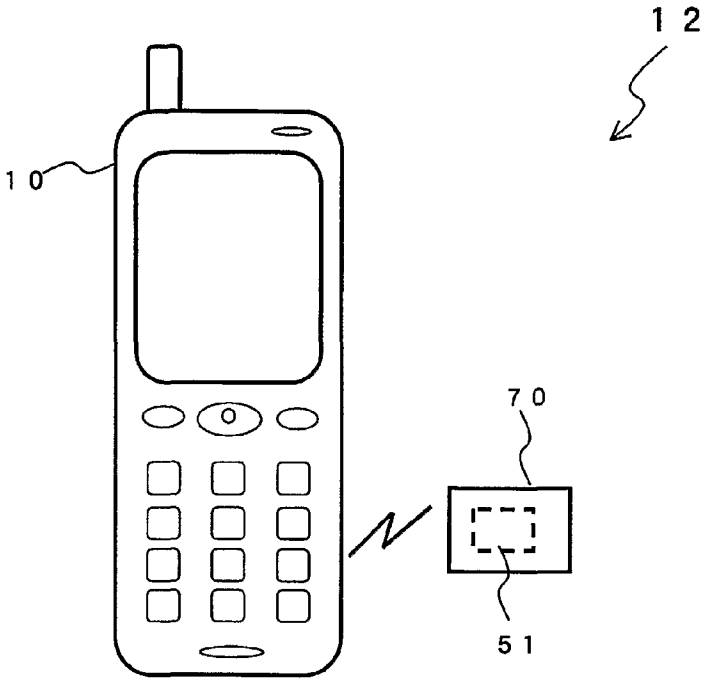
第12図



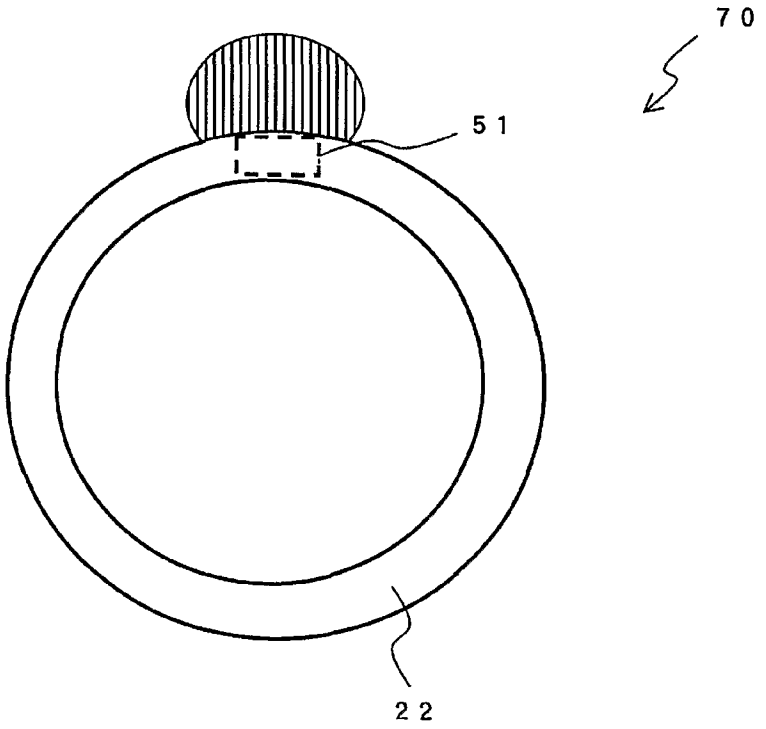
第13図


携帯端末
読み取り装置
S120
カードを選択する。
読み取りコマンドを送受信部へ送る
S220
S121
読み取り要求を受信
送受信部から読み取り要求を発信
S221
S122
選択されているカード情報を発信
カード情報を受信
S222
受信したカード情報は、必要なカード情報か？
S223
YES
NO
S225
エラー
処理の継続
S224
END
END

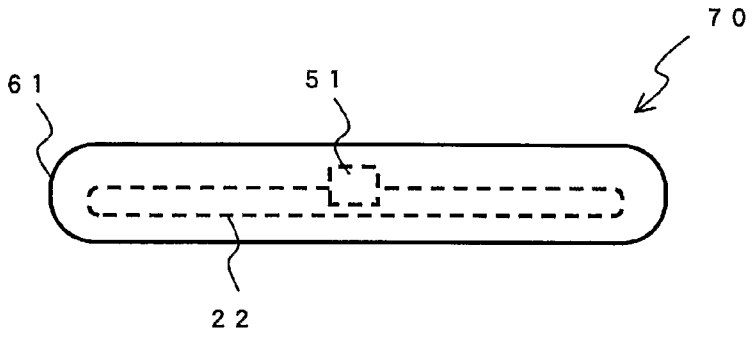
第14図



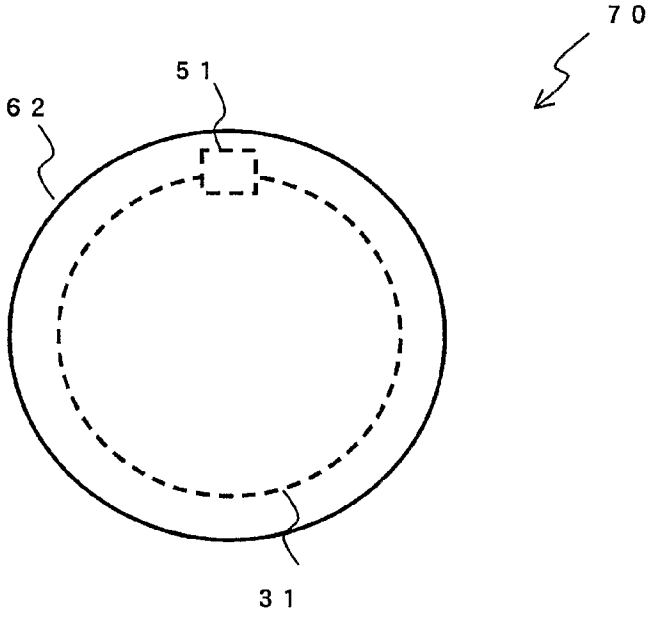
第15図



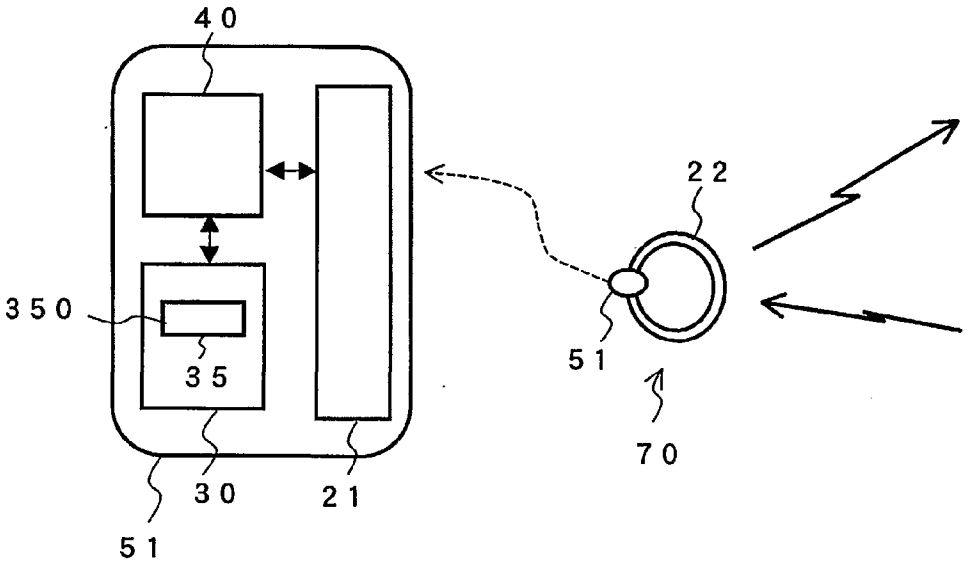
第16図



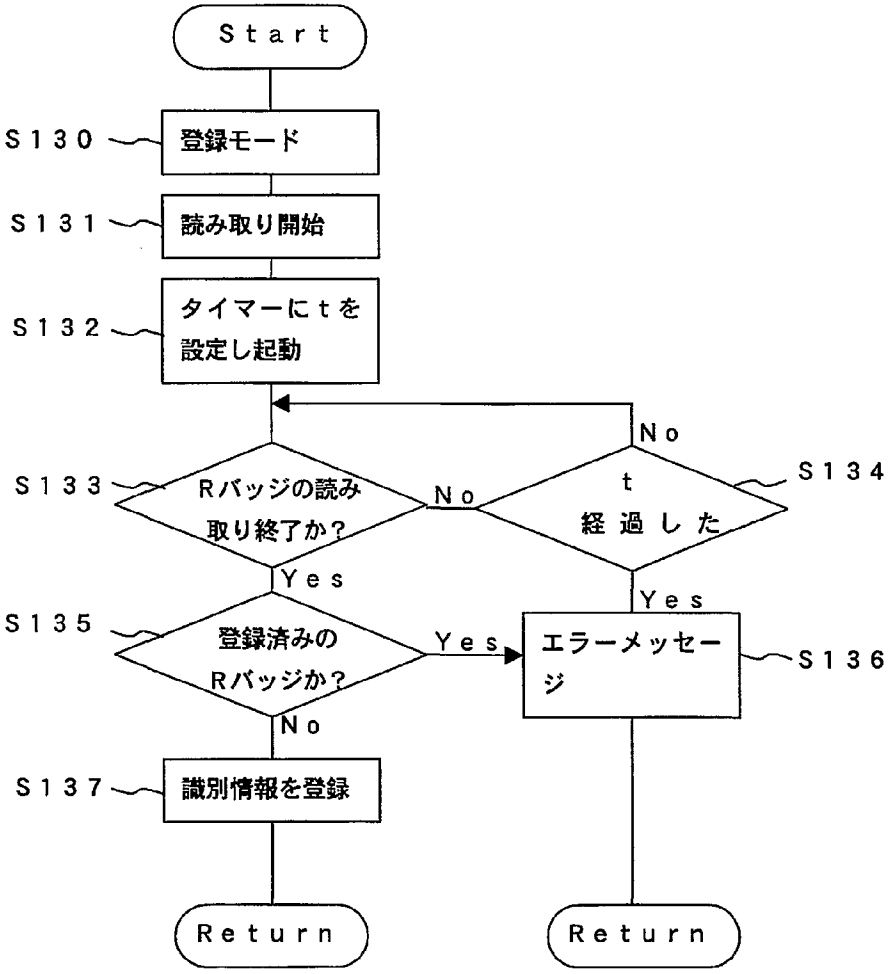
第17図



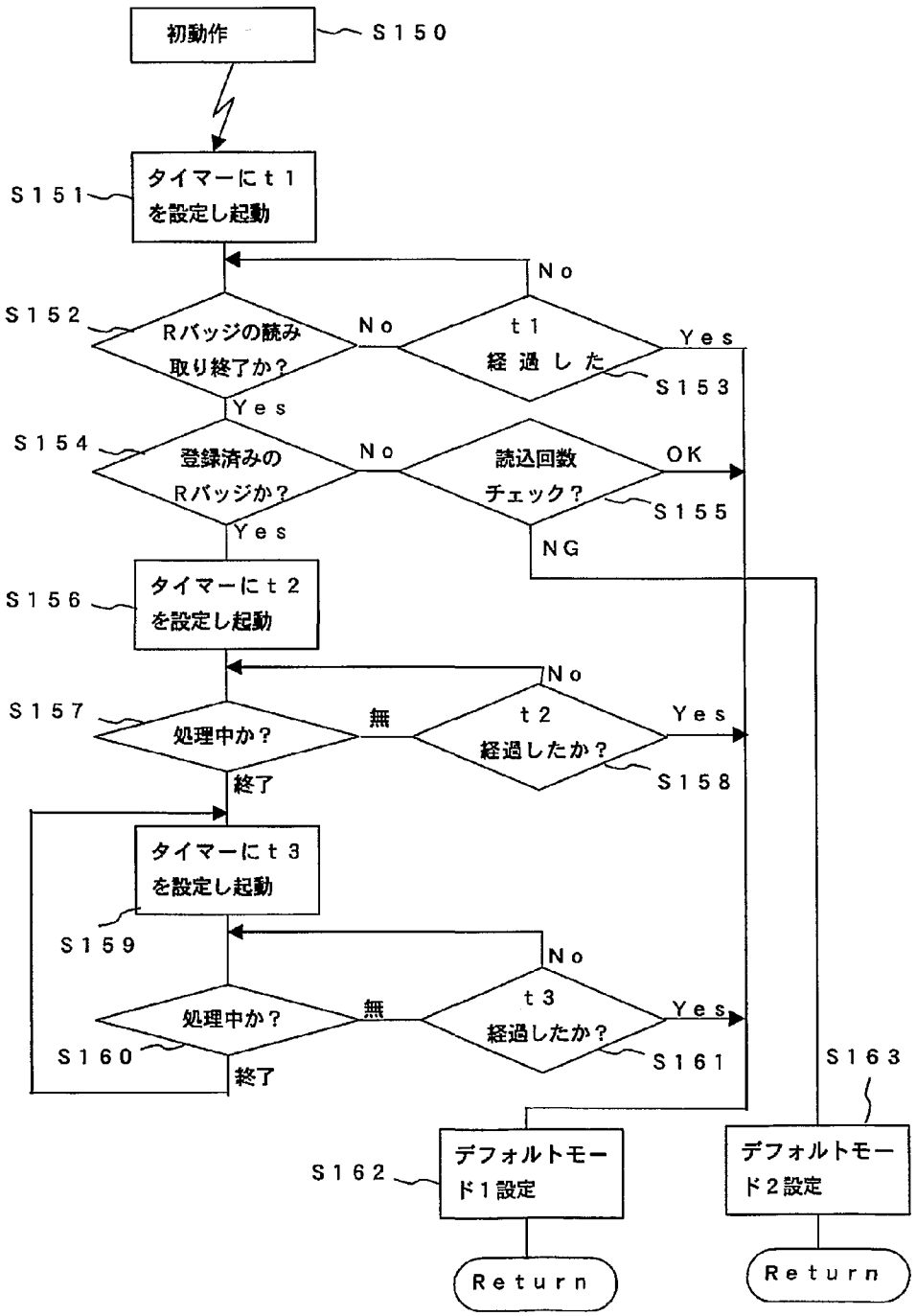
第18図



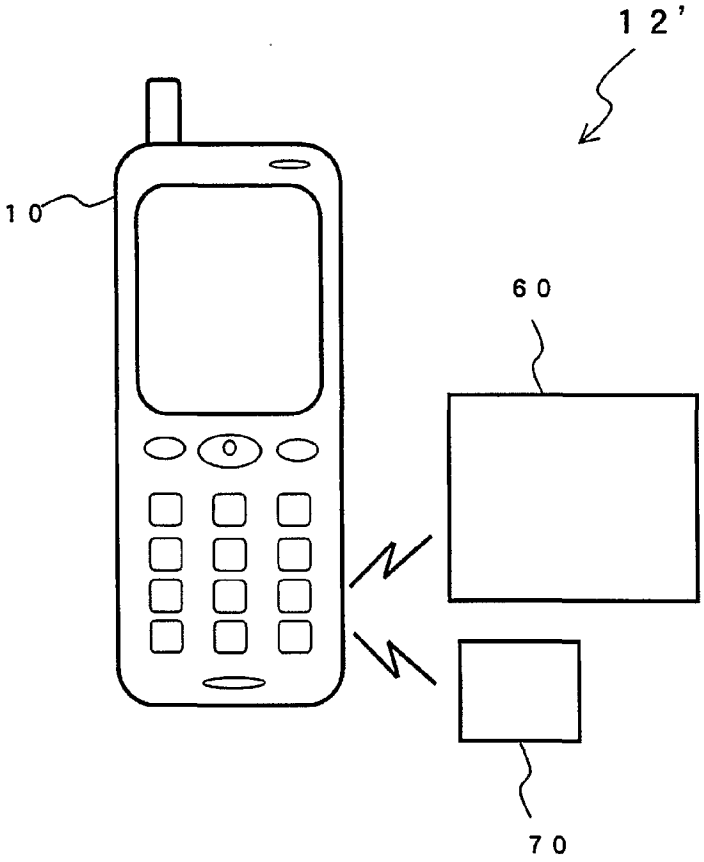
第19図


Start
S130
登録モード
S131
読み取り開始
S132
タイマーにtを設定し起動
S133
Rバッジの読み取り終了か？
No
No
t経過した
S134
Yes
Yes
S135
登録済みのRバッジか？
Yes
エラーメッセージ
S136
No
S137
識別情報を登録
Return
Return

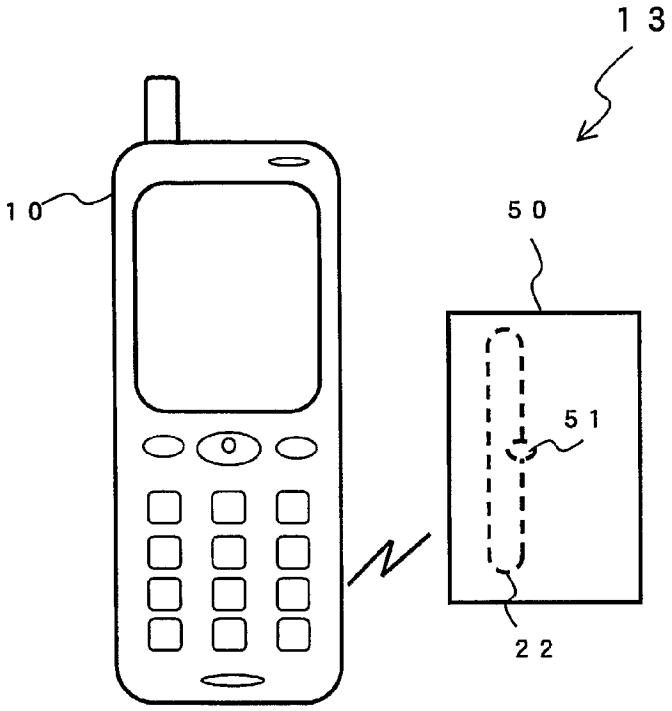
第20図


初動作
S150
タイマーにｔ1を設定し起動
S151
No
S152
Rバッジの読み取り終了か？
No
t1経過した
Yes
S153
Yes
S154
登録済みのRバッジか？
No
読込回数チェック？
OK
S155
Yes
NG
タイマーにｔ2を設定し起動
S156
No
S157
処理中か？
無
t2経過したか？
Yes
S158
終了
タイマーにｔ3を設定し起動
S159
No
処理中か？
無
t3経過したか？
Yes
S160
S161
終了
S163
S162
デフォルトモード1設定
デフォルトモード2設定
Return
Return

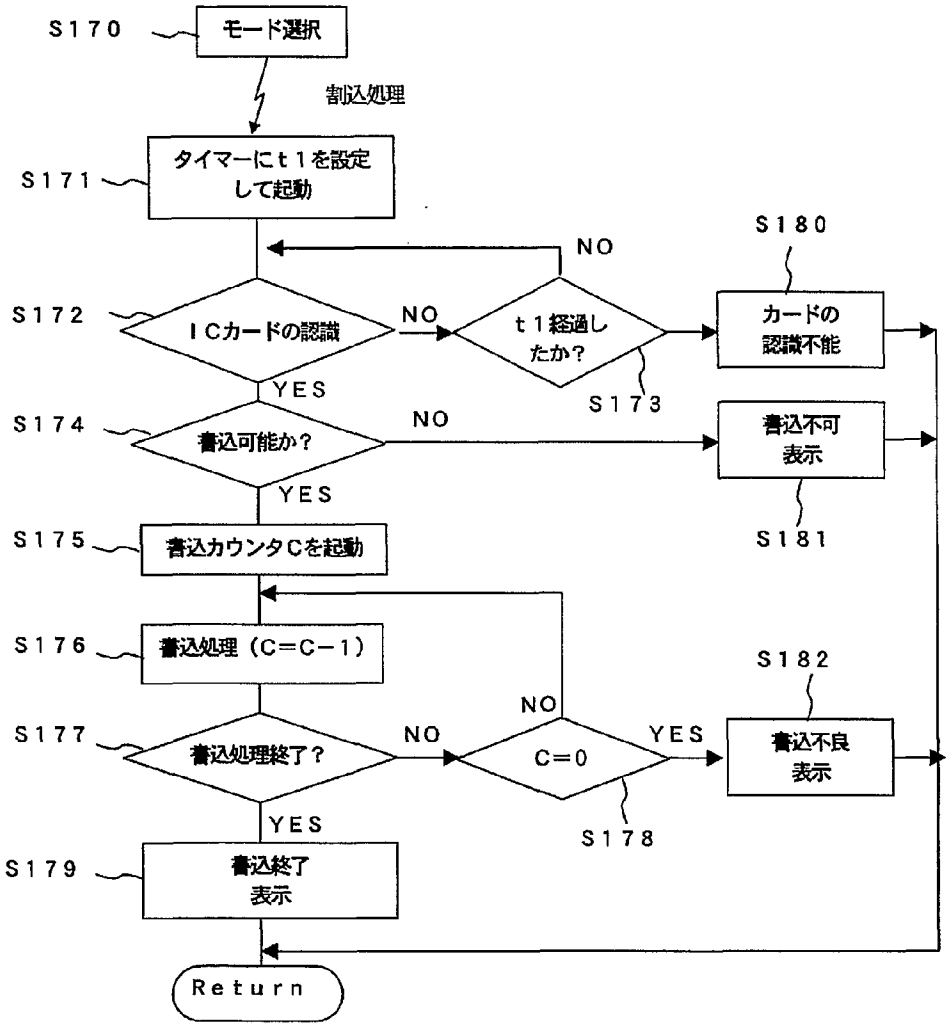
第21図



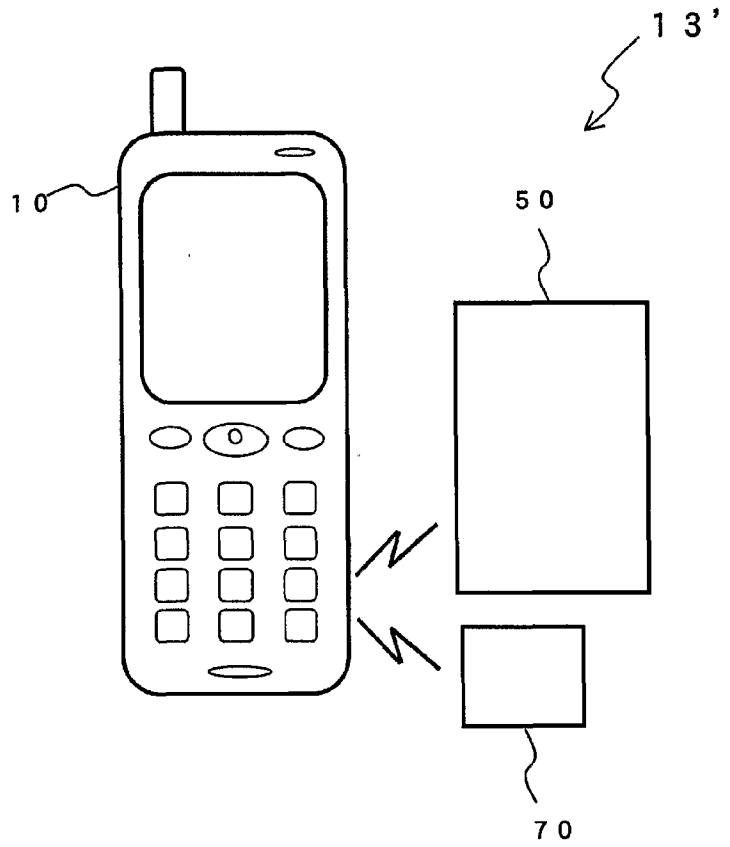
第22図



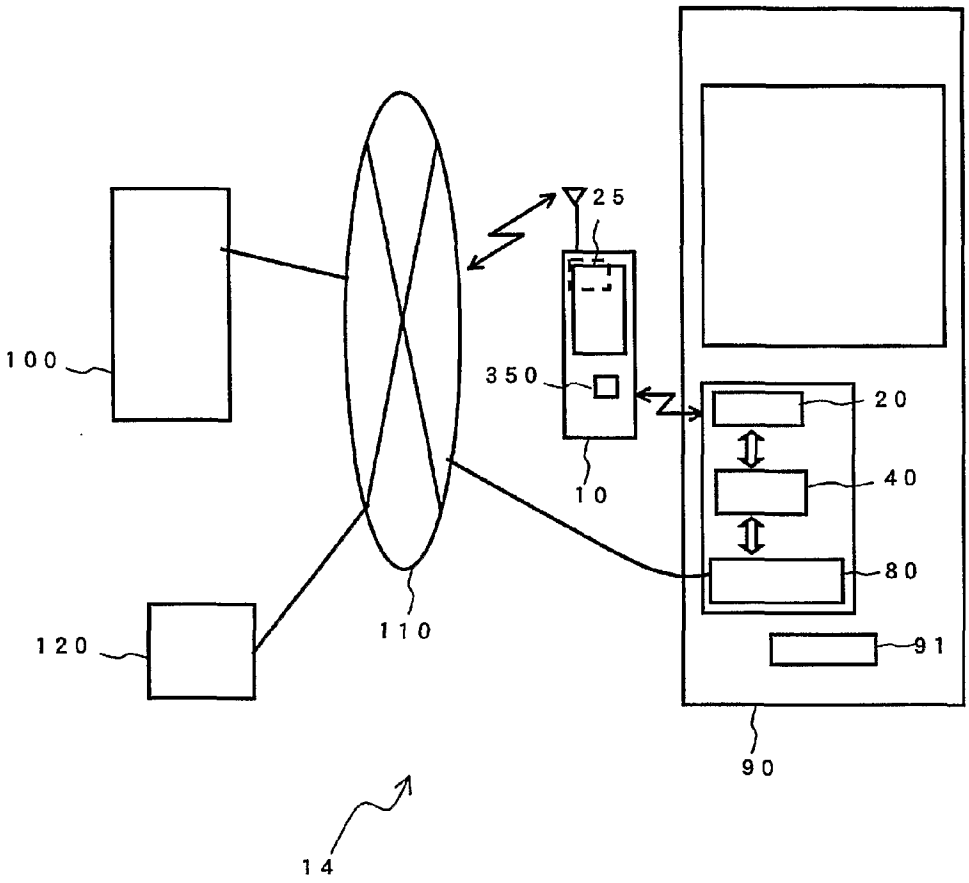
第23図


S170
モード選択
割込処理
S171
タイマーにｔ１を設定して起動
S172
ＩＣカードの認識
NO
ｔ１経過したか?
S173
S180
カードの認識不能
YES
S174
書込可能か?
NO
書込不可表示
S181
YES
S175
書込カウンタＣを起動
S176
書込処理（C=C−1）
S177
書込処理終了?
NO
C=0
YES
S178
S182
書込不良表示
YES
S179
書込終了表示
Return

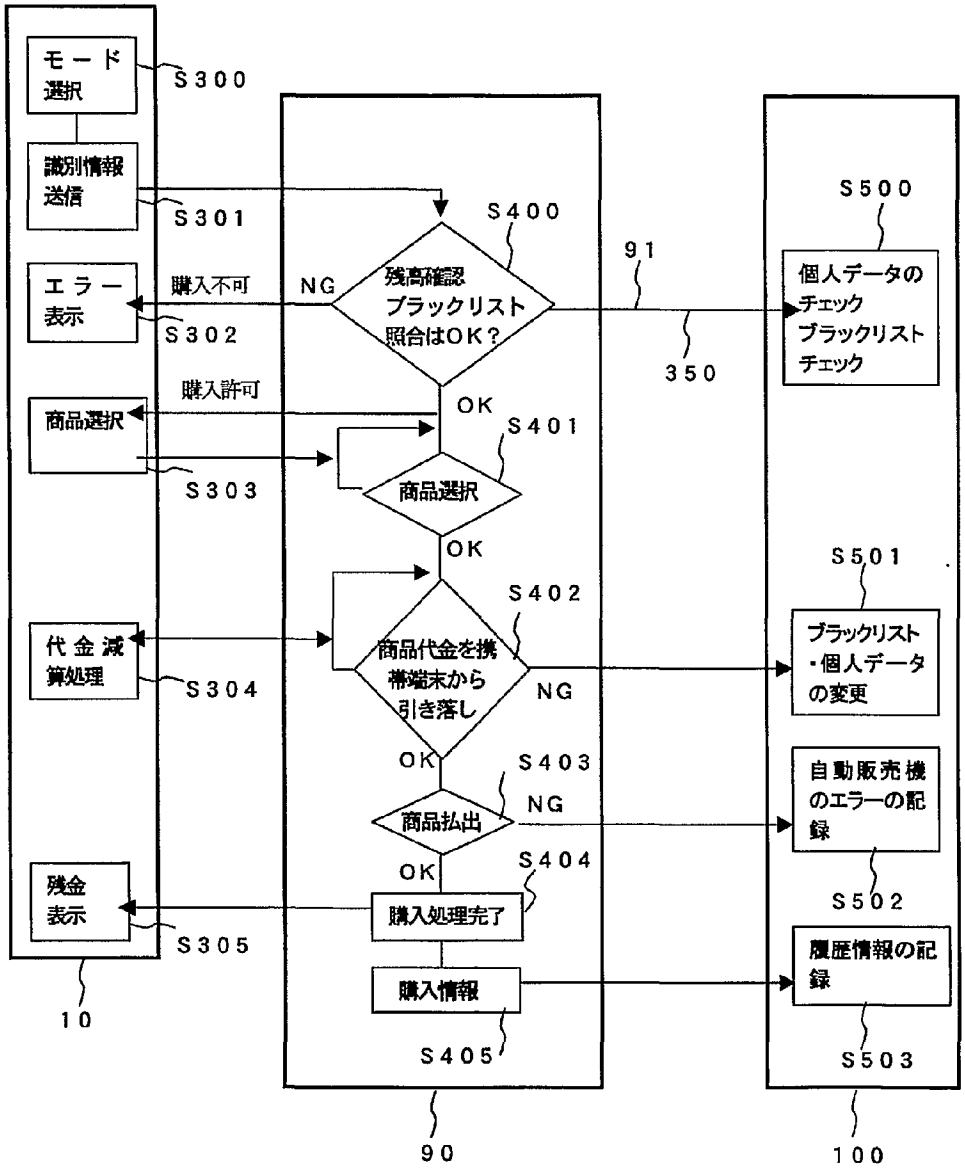
第24図



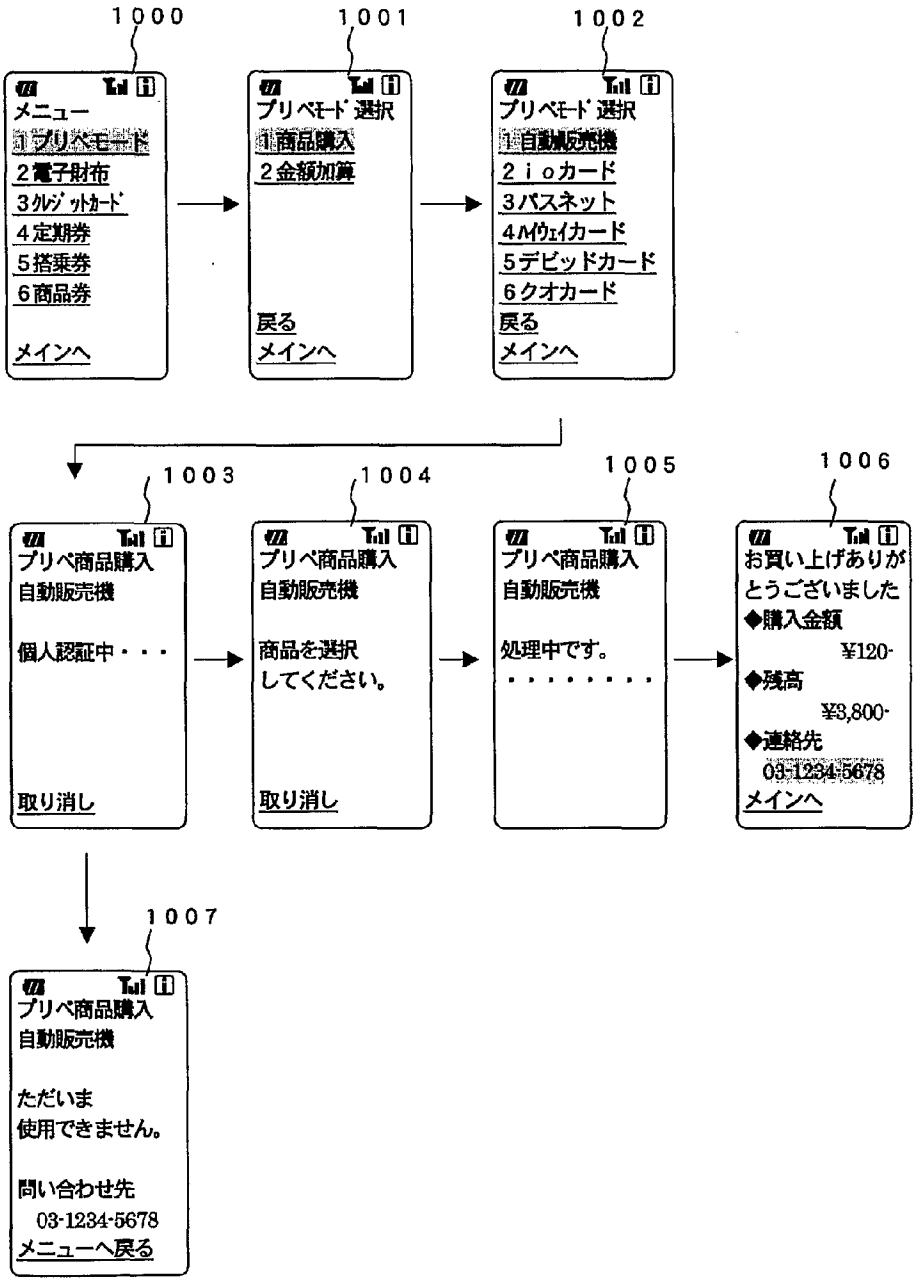
第25図



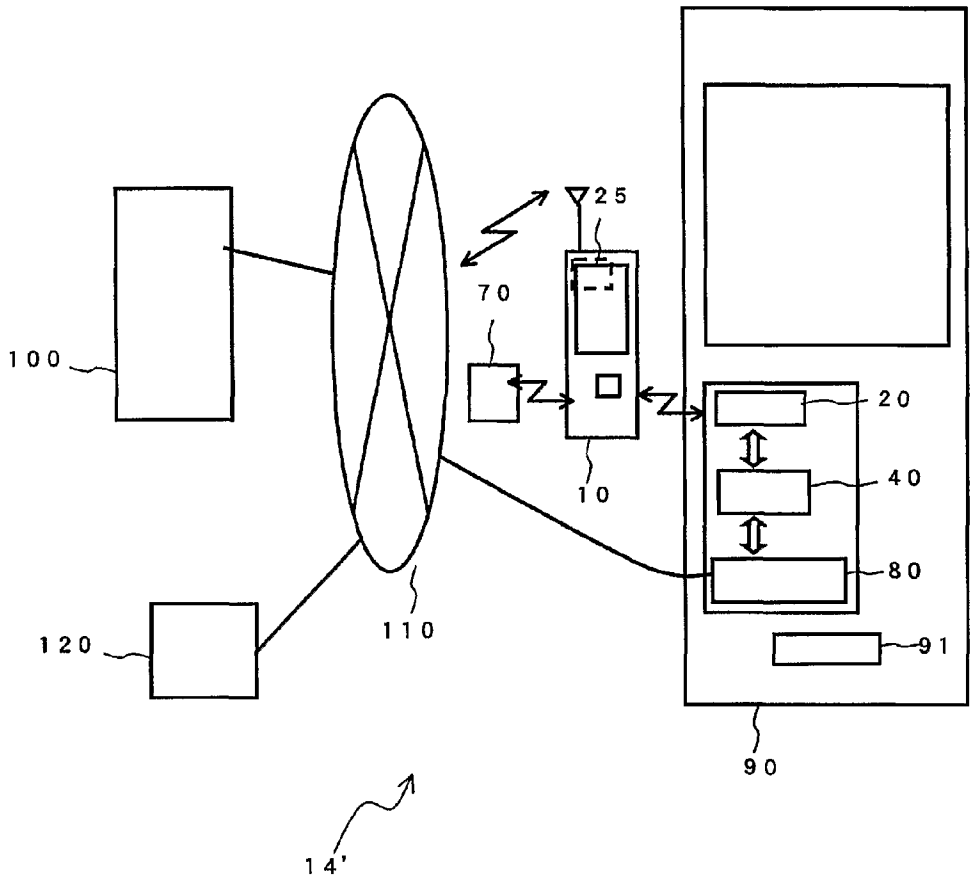
第26図


モード選択
S300
識別情報送信
S301
エラー表示
購入不可
S302
商品選択
購入許可
S303
代金減算処理
S304
残金表示
S305
10
NG
残高確認ブラックリスト照合はOK?
S400
OK
S401
商品選択
OK
S402
商品代金を携帯端末から引き落し
NG
OK
S403
商品払出
NG
OK
S404
購入処理完了
購入情報
S405
90
91
350
S500
個人データのチェックブラックリストチェック
S501
ブラックリスト・個人データの変更
自動販売機のエラーの記録
S502
履歴情報の記録
S503
100

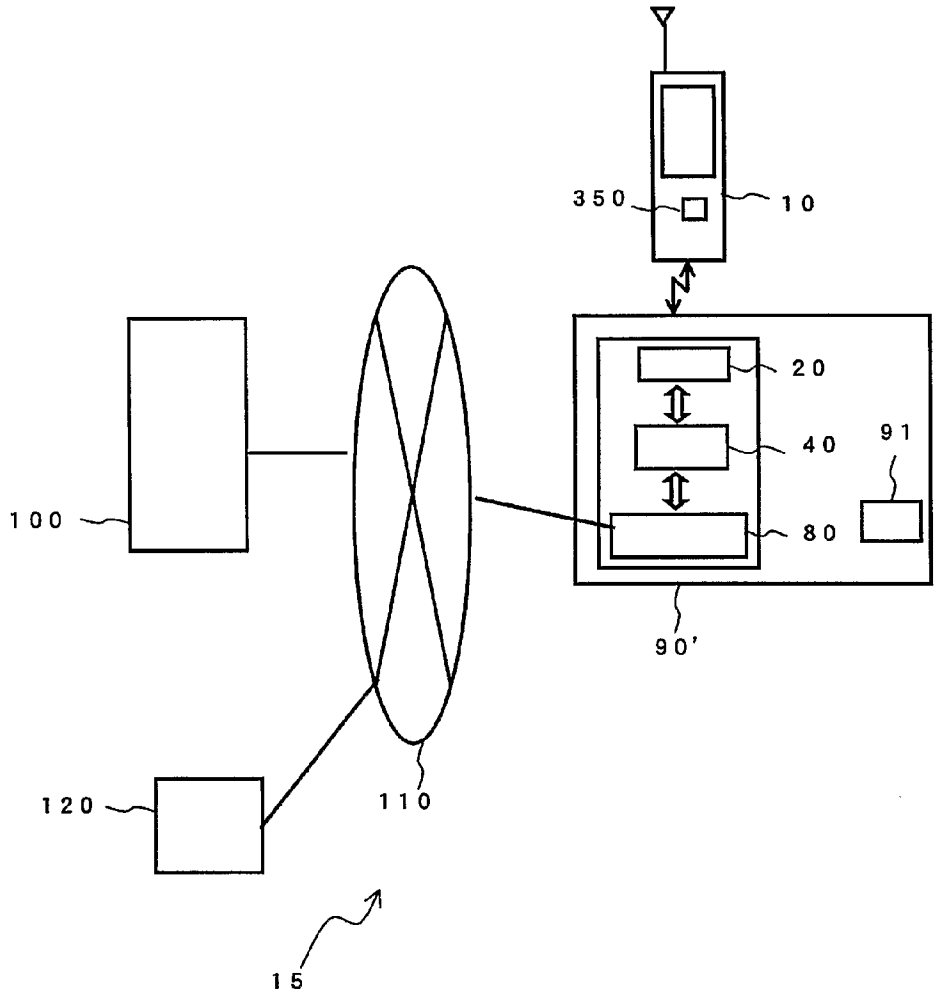
第27図


1000
メニュー
1プリペモード
2電子財布
3クレジットカード
4定期券
5搭乗券
6商品券
メインへ
1001
プリペモード選択
1商品購入
2金額加算
戻る
メインへ
1002
プリペモード選択
1自動販売機
2ｉｏカード
3パスネット
4Mウェイカード
5デビッドカード
6クオカード
戻る
メインへ
1003
プリペ商品購入
自動販売機
個人認証中・・・
取り消し
1004
プリペ商品購入
自動販売機
商品を選択
してください。
取り消し
1005
プリペ商品購入
自動販売機
処理中です。
・・・・・・・・
1006
お買い上げありが
とうございました
◆購入金額
¥120-
◆残高
¥3,800-
◆連絡先
03-1234-5678
メインへ
1007
プリペ商品購入
自動販売機
ただいま
使用できません。
問い合わせ先
03-1234-5678
メニューへ戻る

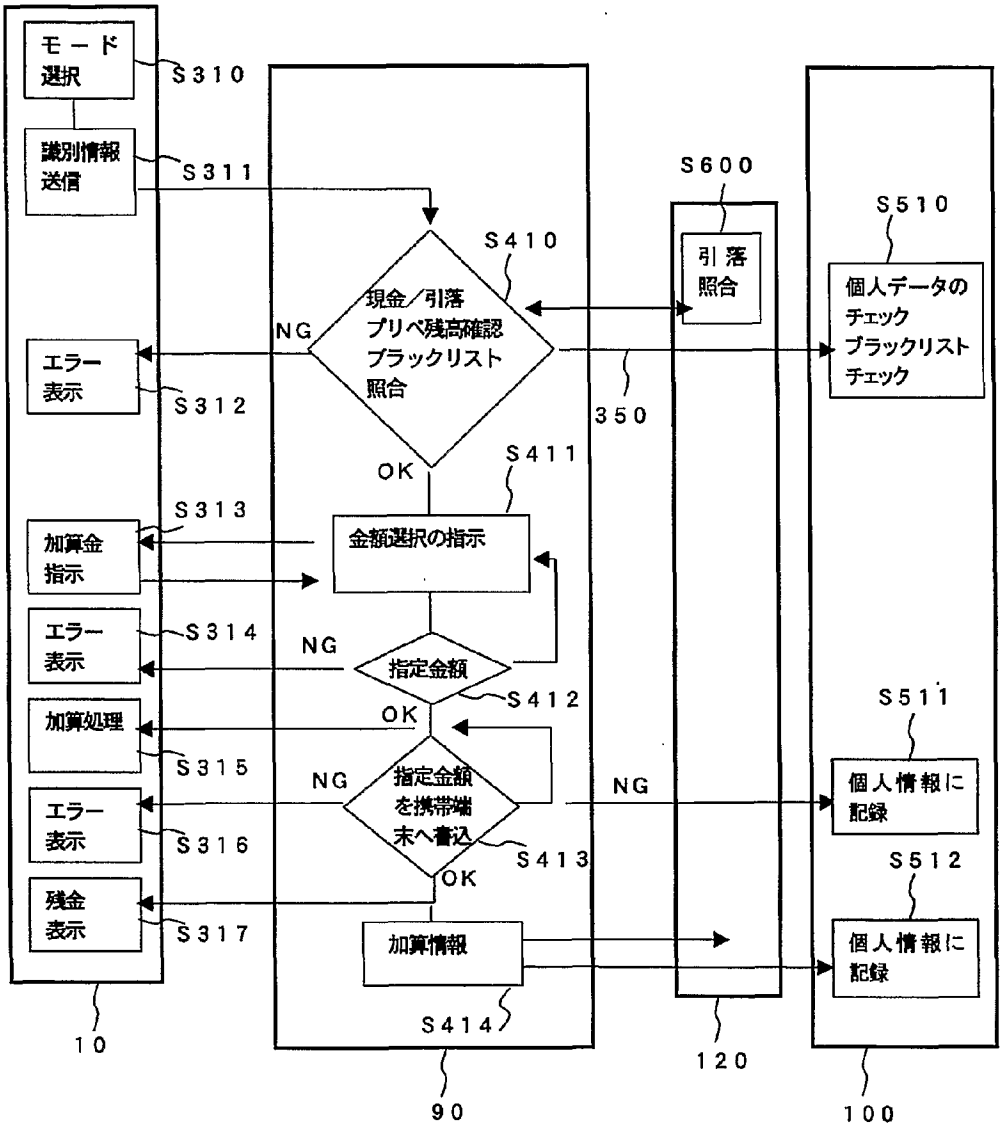
第28図



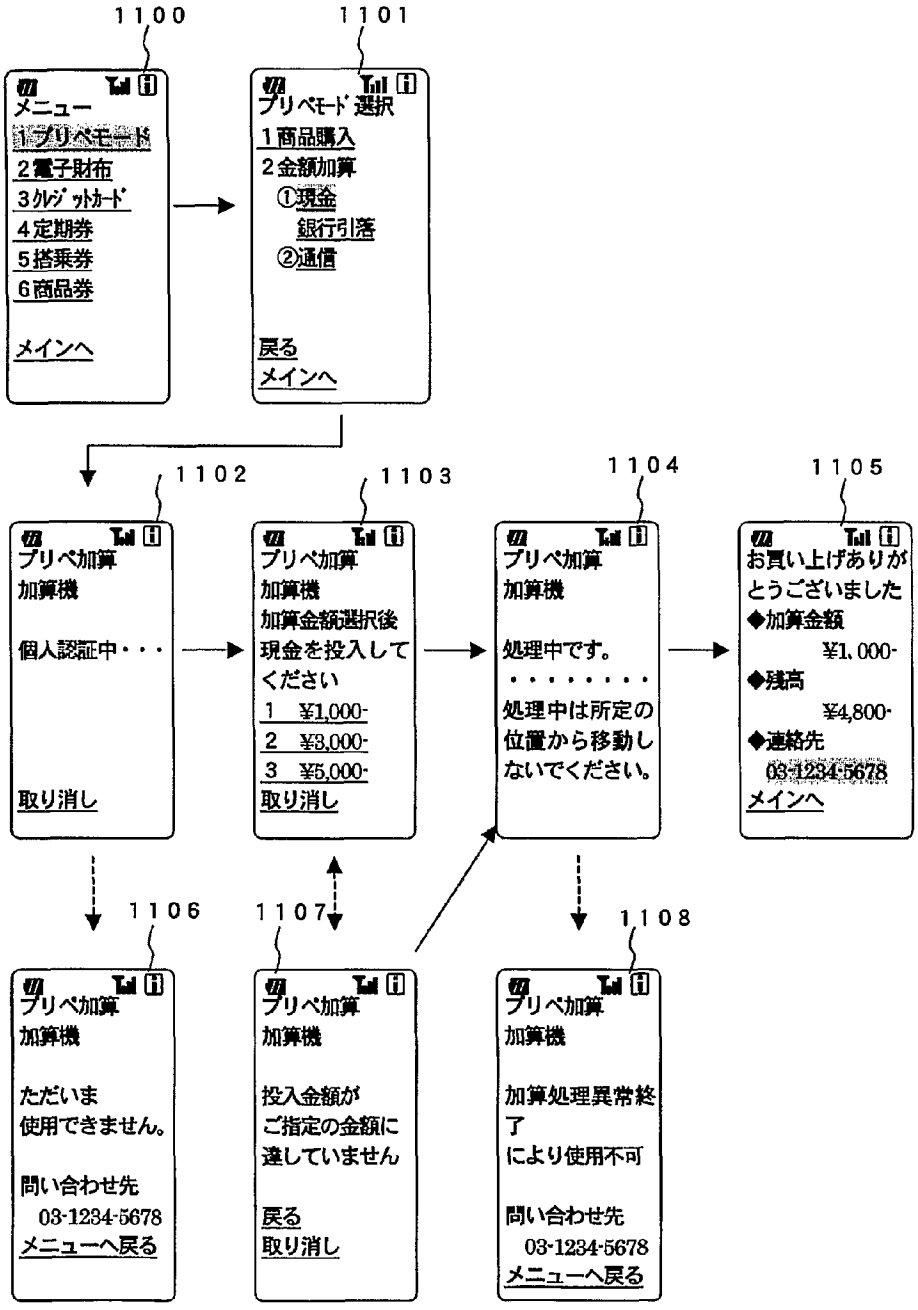
第29図



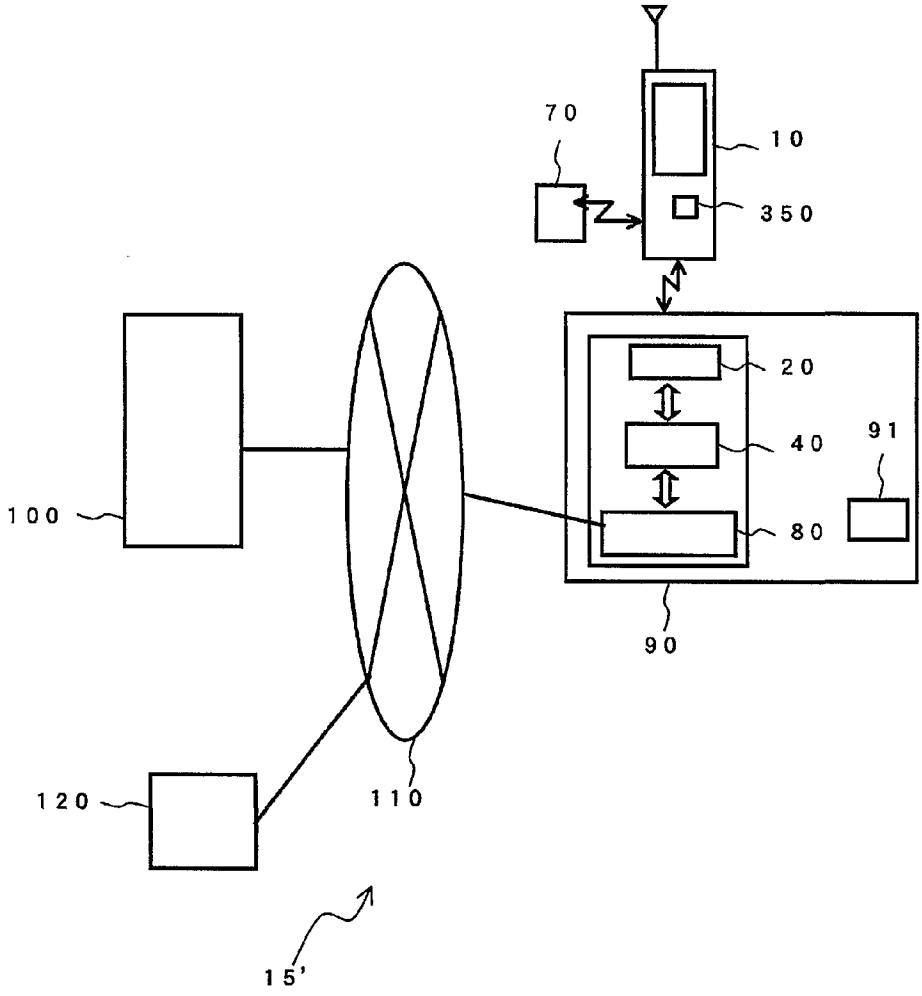
第30図


モード選択
S310
識別情報送信
S311
エラー表示
S312
NG
現金／引落プリペ残高確認ブラックリスト照合
S410
OK
S411
金額選択の指示
S313
加算金指示
エラー表示
S314
NG
指定金額
S412
OK
加算処理
S315
NG
指定金額を携帯端末へ書込
S413
OK
エラー表示
S316
残金表示
S317
加算情報
S414
10
90
350
S600
引落照合
120
S510
個人データのチェックブラックリストチェック
S511
個人情報に記録
S512
個人情報に記録
100

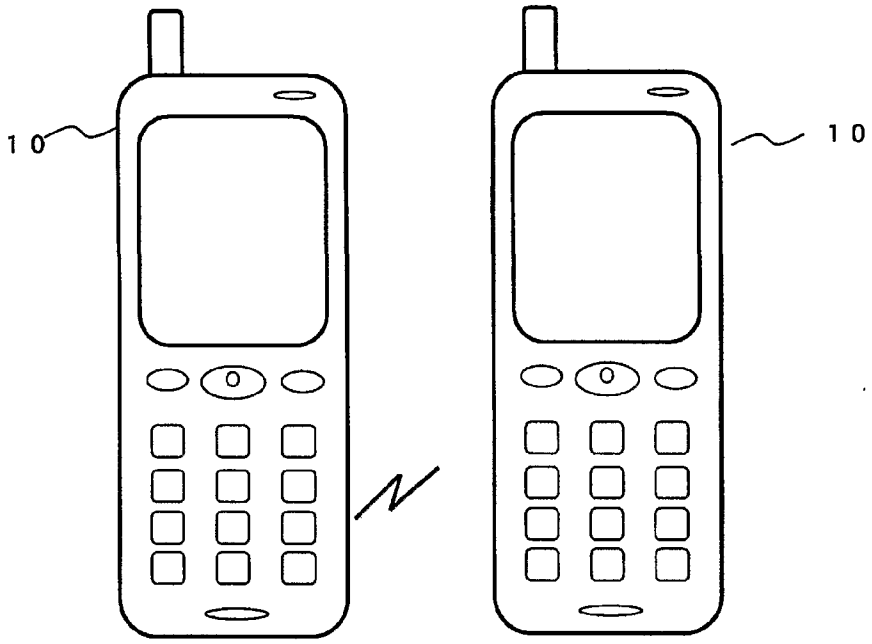
第31図


1100
1101
メニュー
1プリペモード
2電子財布
3クレジットカード
4定期券
5搭乗券
6商品券
メインへ
プリペモード選択
1商品購入
2金額加算
①現金
銀行引落
②通信
戻る
メインへ
1102
1103
1104
1105
プリペ加算
加算機
個人認証中・・・
取り消し
プリペ加算
加算機
加算金額選択後
現金を投入して
ください
1 ¥1,000-
2 ¥3,000-
3 ¥5,000-
取り消し
プリペ加算
加算機
処理中です。
・・・・・・・・
処理中は所定の
位置から移動し
ないでください。
お買い上げありが
とうございました
◆加算金額
¥1,000-
◆残高
¥4,800-
◆連絡先
03-1234-5678
メインへ
1106
1107
1108
プリペ加算
加算機
ただいま
使用できません。
問い合わせ先
03-1234-5678
メニューへ戻る
プリペ加算
加算機
投入金額が
ご指定の金額に
達していません
戻る
取り消し
プリペ加算
加算機
加算処理異常終
了
により使用不可
問い合わせ先
03-1234-5678
メニューへ戻る

第32図



第33図



第34図

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/03789

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06K17/00, 19/073, G06F12/14, 15/00, H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06K17/00, 19/00-19/18, G06F12/14, 15/00, H04Q7/38, H04M1/667

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Jitsuyo Shinan Toroku Koho	1996-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 4-306760 A (Nippon Telegraph And Telephone Corp.), 29 October, 1992 (29.10.92), Full text; all drawings (Family: none)	1-32
Y	JP 9-98480 A (Sanyo Electric Co., Ltd.), 08 April, 1997 (08.04.97), Full text; all drawings (Family: none)	1-32
Y	JP 6-320891 A (Obayashi Corp.), 22 November, 1994 (22.11.94), Full text; all drawings (Family: none)	1-32

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 22 July, 2002 (22.07.02)	Date of mailing of the international search report 06 August, 2002 (06.08.02)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/03789

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 4-155471 A (Oki Electric Industry Co., Ltd., NTT Data Communications Systems Corp.), 28 May, 1992 (28.05.92), Full text; Fig. 5 (Family: none)	3,6,17,20
Y	JP 9-64967 A (NEC Saitama Kabushiki Kaisha), 07 March, 1997 (07.03.97), Full text; all drawings (Family: none)	31,32
Y	JP 3-60543 A (NEC Corp.), 15 March, 1991 (15.03.91), Full text; all drawings & GB 9013610 A0 & GB 2234883 A & US 5212810 A1 & JP 2952898 B	31,32

国際調査報告

国際出願番号　PCT／JP02／03789

A.　発明の属する分野の分類（国際特許分類（IPC））
Int.Cl[7]　G06K17／00，19／073
G06F12／14，15／00
H04Q7／38

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））
Int.Cl[7]　G06K17／00，19／00－19／18
G06F12／14，15／00
H04Q7／38，H04M1／667

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1922－1996年
日本国公開実用新案公報　1971－2002年
日本国登録実用新案公報　1994－2002年
日本国実用新案登録公報　1996－2002年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 4-306760 A(日本電信電話株式会社) 1992.10.29,全文,全図(ファミリーなし)	1-32
Y	JP 9-98480 A(三洋電機株式会社) 1997.04.08,全文,全図(ファミリーなし)	1-32
Y	JP 6-320891 A(株式会社大林組) 1994.11.22,全文,全図(ファミリーなし)	1-32

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
22．07．02	06.08.02

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	奥村　元宏	5N	8022
	電話番号　03－3581－1101　内線　3545		

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０２／０３７８９

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 4-155471 A(沖電気工業株式会社,エヌ・テイ・テイ・データ通信株式会社) 1992.05.28,全文,第５図 (ファミリーなし)	3,6,17,20
Y	JP 9-64967 A(埼玉日本電気株式会社) 1997.03.07,全文,全図(ファミリーなし)	31,32
Y	JP 3-60543 A(日本電気株式会社) 1991.03.15,全文,全図 & GB 9013610 A0 & GB 2234883 A & US 5212810 A1 & JP 2952898 B	31,32